Bezpečnostní audit IT ve společnosti Popron systems s.r.o

Security audit of IT in Popron systems ltd.

Bc. Aleš Klabal

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Aleš KLABAL**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní audit IT ve společnosti Popron systems s.r.o.**

Zásady pro vypracování:

1. **Proveďte průzkum současných trendů a moderních postupů v oblasti bezpečnostního auditu u firem, které se zaměřují na tento obor podnikání.**
2. **Na základě analýzy stanovte jednu metodu dle, které se provádí bezpečnostní audit, na tuto se zaměřte a vypracujte popis principů, legislativ a norem, kterými se řídí.**
3. **Na Vámi vybraném podnikatelském subjektu proveďte bezpečnostní audit s detailním zaměřením na jeho nejdůležitější části, které rozpracujte.**
4. **Na základě syntézy z Vámi provedeného auditu stanovte oblasti, jejichž současné řešení nevyhovuje doporučeným standardům a normám, navrhněte kroky vedoucí k jejich nápravě.**

Rozsah práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **KOPÁČIK, Ivan, et al. Management and audit of Information security : Manual for Manager. Brtatislava, Slovensko : Sineal s.r.o., 2007. 322 s. ISBN 978-80-969747-0-2.**
2. **DOSEDĚL , Tomáš. Počítačová bezpečnost a ochrana dat. Libor Pácl. Brno : Computer press, c2004. 187 s. ISBN 80-251-0106-1.**
3. **DOUCEK, P.: Bezpečnost informační systémů a její prosazování v České republice, In: Informatika 2003, pp. 141 -- 146, Bratislava 2003, ISBN 80-233-0491-7.**
4. **SVATÁ, V.: Audit informačního systému, VŠE Praha, 2007, ISBN 80-245-0975-X**
5. **POUR, Jan. Informační systémy a technologie. 1.vyd Edice učebních textů 2006. ISBN 80-86730-03-4**
6. **VRANA, Ivan a RICHTA, Karel. Zásady a postupy zavádění podnikových informačních systémů: Praktická příručka pro podnikové manažery. 1. vyd. Praha : Grada, 2005. 187 s. ISBN 80-247-1103-6**
7. **HANÁČEK, Petr a STAUDEK, Jan. Bezpečnost informačních systémů, Úřad pro státní bezpečnostní systém 2000**
8. **MOLNÁR, Zdeněk. Automatizované informační systémy. Praha: ČVUT 2000, PLU 2607**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce podává komplexní přehled o teorii a praxi bezpečnostního auditingu v oblasti IT. Nabízí informace o postupech a pravidlech z mezinárodně uznávaných a schválených norem, zabývajících se problematikou řízení bezpečnosti informací. Detailněji popisuje nejefektivnější způsob budování bezpečného IS - metodou PDCA. Praktická část práce pak popisuje průběh bezpečnostního auditu IT v praxi. Autor se podílel na provedení analýzy bezpečnosti systému jedné konkrétní firmy. Tato práce podává zprávu o použitých postupech, dosažených výsledcích a navržených opatřeních v rámci tohoto projektu bezpečnostního auditu.

Klíčová slova:

bezpečnostní audit, norma, řízení bezpečnosti, analýza, směrnice, aktiva, bezpečnostní politika, důvěrnost, integrita, dostupnost, autenticita, management, ISO, ISMS, PDCA

ABSTRACT

The thesis presents a complex overview of theory and praxis of security auditing in IT. It provides information on processes and rules defined in internationally accepted standards of information security management. The most effective method of building secured information system – the PDCA, is described in detail. The practical part of thesis describes the procedure of security audit in praxis. Author took part in analyzing the security of information system in specific company. This thesis gives a report of used procedures, methods and reached results and suggested arrangements made during the project.

Keywords:

Security audit, norm, security management, analysis, directive, assets, security policy, confidence, integrity, availability, authenticity, management, ISO, ISMS, PDCA

Na tomto místě bych rád vyjádřil poděkování doc. Mgr. Romanovi **Jaškovi** Ph.D., vedoucímu mé diplomové práce, za podnětné připomínky a navedení správným směrem. Také bych rád poděkoval všem, kteří mi byli při psaní oporou.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

…….

podpis diplomanta

OBSAH

ÚVOD

V posledních několika letech dochází k velkému rozvoji informačních technologií a jejich konkrétní realizaci v podobě informačních a komunikačních systémů. Tyto systémy přešly od fyzicky centralizované topologie k topologii decentralizované. Distribuováním dat a aplikací na více počítačů vzrůstají nároky na komunikační infrastrukturu, která musí jednotlivá místa zpracování dat propojit a zajistit tak rychlé a bezpečné spojení všech uzlů sítě.

V oblasti bezpečnosti se tento přechod k distribuovanému zpracování dat projevil velmi razantně. Diskuse o zabezpečení informačních systémů se staly tématem dneška. Na počítačové systémy začalo působit mnohem více hrozeb, než při centralizovaném zpracování dat. Vedle klasických fyzických či personálních hrozeb roste ohrožení informačních systémů ze strany neautorizovaných osob zejména při přenosu informace komunikační infrastrukturou.

Vznik této diplomové práce rovněž reaguje na zákonnou povinnost všech organizací zpracovávajících citlivá data, např. personální informace, provozovat své počítačové systémy bezpečným způsobem. Nesmí tedy dojít k úniku důvěrných a osobních informací. Není-li bezpečnost systému zajištěna pomocí vhodných nástrojů umožňujících průběžně kontrolovat požadované bezpečnostní parametry, systém by měl být ve vhodných intervalech pravidelně auditován měřitelným způsobem a to nejlépe třetí stranou nezávislou na administrátorech a managementu informačního systému. Toto testování se snažilo co nejvíce přiblížit podmínkám, které by měl potenciální narušitel. Všechny testy byly provedeny minimálně 3x a s různými nástroji, aby byla co nejvíce snížena možnost lidského selhání. V rámci hodnocení byl proveden sběr dat z používaných aktivních prvků, serverů a pracovních stanic. Během testování nebyly používány techniky, které by mohly způsobit nedostupnost serverů. Během hodnocení nebyla měněna systémová konfigurace nebo soubory hodnocených komponent. Veškeré práce probíhaly za aktivního přispění správce IS. Další upřesňování sesbíraných dat probíhalo telefonicky a mailem.

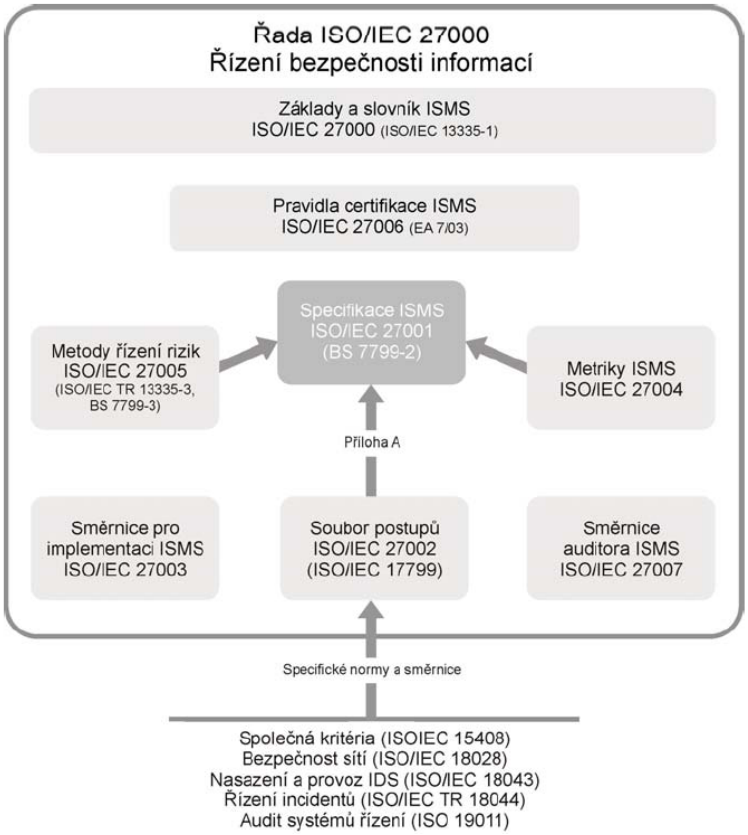
I. TEORETICKÁ ČÁST

1 LEGISLATIVA A NORMY AUDITU IT

V dnešní vysoce vyspělé době informačních technologií již není možné se při auditu těchto vysoce sofistikovaných informačních systémů spoléhat pouze na vlastní zkušenosti a zkušenosti pracovníků v organizaci působící. Dále pak s ohledem na integraci ČR do evropské unie je třeba se přizpůsobit evropským trendům a přijmout pravidla tohoto společenství za vlastní. Z tohoto důvodu byla ve spolupráci s evropskými normalizačními institucemi vyvinuta rodina norem a legislativ, dle které by se měl každý subjekt, který tento audit informačních technologií realizuje řídit. V neposlední řadě slouží tyto normy jako metrika, která zaručuje srovnatelnost a transparentnost s audity prováděnými v jiných společnostech a také mezi auditorskými autoritami navzájem.

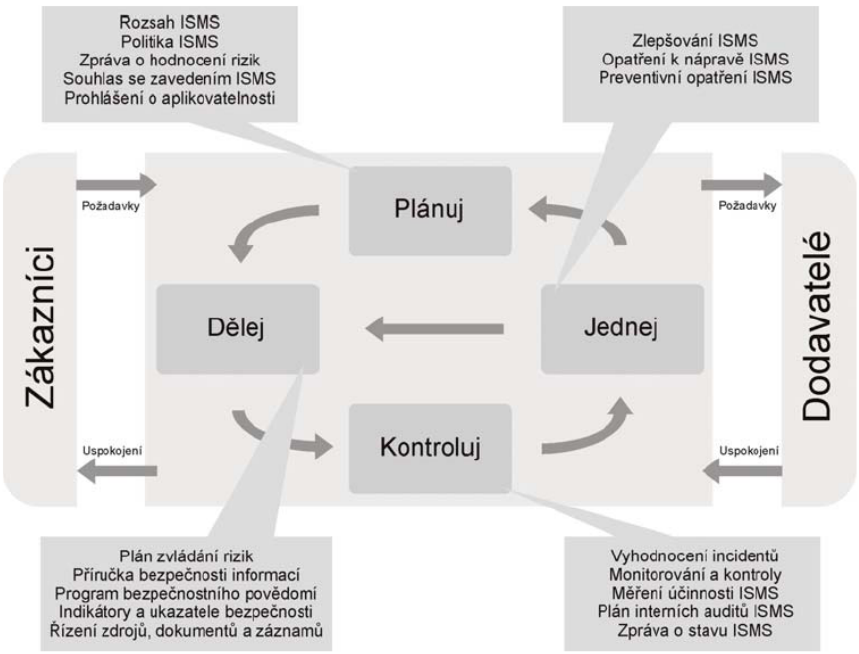
1.1 Mezinárodní normy pro řízení bezpečnosti informací

Na jaře roku 2005 organizace ISO ohlásila zavedení nové řady norem ISO/IEC 27000, která se věnuje problematice řízení bezpečnosti informací.



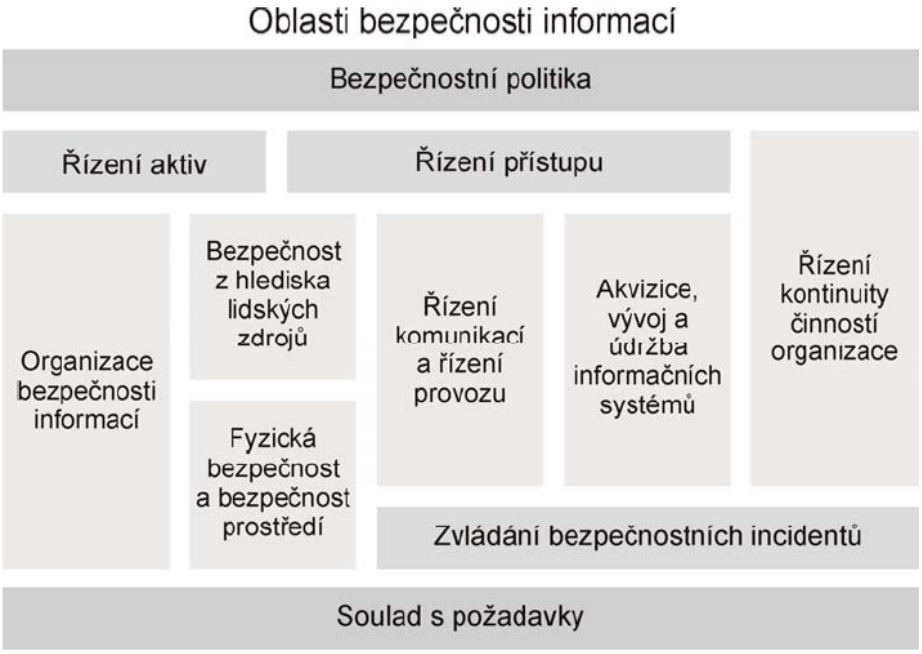
Koncept řady ISO/IEC 27000 Obr. 1 [1]

Nová řada norem pro řízení bezpečnosti informací ISO/IEC 27000 vychází ideově z konceptu PDCA a jejím základem jsou normy, jež jsou uvedeny na obrázku Obr.1. Podobně jako u jiných systémů řízení (např. ISO 9001, ISO 14001) je za jádro normalizace považována definice systému. V případě ISMS se tak stává klíčovým prvkem mezinárodní norma **ISO/IEC 27001:2005 – Information security management system – Requirements (Systém řízení bezpečnosti informací – Požadavky)**, která vychází ze známého britského standardu BS 7799-2 a která byla vydána v říjnu roku 2005. Nosné prvky, které norma vyžaduje pro budování ISMS, jsou vidět na následujícím obrázku.



PDCA Model pro bezpečnost informací Obr. 2 [1]

Druhou nejdůležitější normou této řady je norma **ISO/IEC 27002 – Code of practice for information security management (Soubor postupů pro řízení bezpečnosti informací)**, která obsahuje podrobný výklad vhodných bezpečnostních opatření. Tato norma byla vydána již v polovině roku 2005 a to ještě s označením ISO/IEC 17799:2005. Ta obsahuje tzv. nejlepší praxi řízení bezpečnosti informací a doporučení normy definuje 133 bezpečnostních opatření, která jsou rozdělena do 11 oblastí (viz následující obrázek).



Oblasti bezpečnosti informací Obr. 3 [2]

Na začátku roku 2009 byl spuštěn proces aktualizace obou norem (tj. ISO/IEC 27001 a ISO/IEC 27002), který bude uzavřen v roce 2011 vydáním nových verzí. Od počátku roku 2007 se dalším přírůstkem řady ISO/IEC 27000 stala norma **ISO/IEC 27006 – Requirements for the accreditation of bodies providing certification of information security management systems** (Požadavky na akreditaci orgánů provádějících certifikaci systémů řízení bezpečnosti informací) [4]. Ta upřesňuje pravidla pro udělování certifikací ISMS a podle ní musí postupovat certifikační orgány, které služby spojené s certifikací ISMS poskytují. Norma nahradila již poměrně zastaralý evropský dokument EA 7/03 z roku 2000. Poslední již vydanou je **ISO/IEC 27005:2008 – Information security risk management (Řízení rizik bezpečnosti informací)** [5], která podrobně definuje pravidla a postupy řízení rizik a nahradila již zastaralou normu ISO/IEC TR 13335-3. Kromě doporučení spojených s řízením rizik tato norma obsahuje i rozsáhlé katalogy hrozeb a zranitelností. Novými příspěvky řady ISO/IEC 27000 by se v blízké budoucnosti mělo stát několik dalších mezinárodních norem. Mezi prvními by měla být norma **ISO/IEC 27004 – Information security management measurements (Měření účinnosti řízení bezpečnosti informací)** [3], která upřesní pravidla a způsoby využití nástrojů pro sledování účinnosti a efektivnosti zavedení a prosazení ISMS. Norma především předepisuje strukturu ukazatelů pro měření ISMS, upřesňuje pravidla pro definici a využívání bezpečnostních ukazatelů a

doporučuje některé obecné ukazatele pro sledování účinnosti ISMS. Mezi nimi by se měla objevit norma **ISO/IEC 27000 – Information security management system fundamentals and vocabulary (Základy a slovník systému řízení bezpečnosti informací)**, jejímž úkolem je sjednotit odborný slovník a definovat základní modely uplatňované při řízení bezpečnosti informací. Tato norma nahradí ISO/IEC 13335-1 a tím zanikne řada ISO/IEC 13335. Novou normou bude **ISO/IEC 27003 – Information security management system implementation guidance (Směrnice pro implementaci systému řízení bezpečnosti informací)**. Ta bude obsahovat doporučení a návody, které jsou pro zaváděním ISMS sice vhodné, nicméně nemají podobu závazných pravidel. Posledním, v současnosti známým příspěvkem řady ISO/IEC 27000, by se měla stát norma **ISO/IEC 27007 – ISMS Auditor Guidelines (Směrnice auditora ISMS)**, která by měla upřesnit pravidla a postupy spojené s prováděním interních i externích auditů ISMS. Během několika málo let by celá řada ISO/IEC 27000 měla obsahovat devět následujících dokumentů:

- ISO/IEC 27000 – Základy a slovník pro systém řízení bezpečnosti informací (rok vydání 2009),
- ISO/IEC 27001:2005 – Systém řízení bezpečnosti informací – Požadavky (vydáno v říjnu 2005 a jako ČSN v říjnu 2006),
- ISO/IEC 27002:2005 (dříve označovaná jako ISO/IEC 17799:2005) – Soubor postupů pro řízení bezpečnosti informací (vydáno v červnu 2005 a jako ČSN v srpnu 2006),
- ISO/IEC 27003 – Příručka pro zavádění systému řízení bezpečnosti informací
- ISO/IEC 27004 – Měření řízení bezpečnosti informací
- ISO/IEC 27005:2008 – Řízení rizik bezpečnosti informací (vydáno v červnu 2008 a jako ČSN v tisku),
- ISO/IEC 27006:2007 – Pravidla certifikace ISMS (vydáno v únoru 2007),
- ISO/IEC 27007 – Směrnice auditora ISMS (vydání je plánováno na rok 2010),
- ISO/IEC TR 27008 – Příručka pro audity o opatřeních ISMS (vydání je plánováno na rok 2012).

Kromě nich jsou v současné době připravovány další dokumenty této řady. Jejich názvy jsou velmi často pracovní, a proto jsou uvedeny pouze v anglickém originále. Jedná se o následující normy, které by se měli věnovat doporučení a výkladu ISMS pro specifické použití:

- ISO/IEC 27010 – Information security management for inter-sector communications (vydání je plánováno na rok 2011),
- ISO/IEC 27011:2008 – Information security management guidelines for telecommunications,
- ISO/IEC 27012 – Information security management guidelines for e-government services (vydání je plánováno na rok 2011),
- ISO/IEC 27013 – Guidance on the integrated implementation of 20000-1 and 27001 (realizace projektu je zvažována),
- ISO/IEC 27014 – Information security governance framework (realizace projektu je zvažována),
- ISO/IEC 27015 – Information security management guidelines for financial and insurance services (realizace projektu je zvažována),
- ISO/IEC 27799:2008 - Security Management in Health using ISO/IEC 27002.

Kromě doporučení pro specifické použití ISMS jsou připravovány normy, které se budou podrobněji věnovat určitým bezpečnostním okruhům. Jedná se především o následující normy:

- ISO/IEC 27031 – Specification for ICT Readiness for Business Continuity (tato norma bude navazovat na britské normy BS 25999 – Business Continuity Management resp. BS 25777 Information and communication technology continuity management – Code of Practice, která byla postupně vydána v letech 2006 až 2008)
- ISO/IEC 27032 – Guidelines for cybersecurity,
- ISO/IEC 27033 – IT network security (nahradí všechny díly ISO/IEC 18028),

- ISO/IEC 27034 – Application security,
- ISO/IEC 27035 – Information Security Incident Management (nahradí ISO/IEC TR 18044).

Směr rozvoje bezpečnostních standardů je patrný ze vzniku dalších rodin norem. Jedná se o rodinu norem ISO/IEC 29000, která se zabývá problematikou **soukromí (Privacy)** a o rodinu norem ISO/IEC 24000 a ISO/IEC 19000, které se zabývají novými trendy v řízení přístupů k aktivům informačních systémů – **biometrikou (Biometrics)**.

Další, nově vznikající, rodinou norem je ISO/IEC 31000, jejímž obsahem je řízení rizik na obecné úrovni. S ní potom musí být harmonizovány speciální normy pro řízení rizik jako např. ISO/IEC 27005.

Všechny tyto rodiny norem pak mají vazby na ostatní rodiny norem, které vymezují integrovaný systém řízení ISO 9000 a ISO 14000.

2 METODIKA BEZPEČNÉHO IT VE SPOLEČNOSTI

2.1 PDCA

Cyklus PDCA byl původně vytvořen Walterem Shewhartem v roce 1930. Následně PDCA pro zlepšování jakosti využil a rozpracoval Edwards Deming. Zkratka PDCA vznikla spojením počátečních písmen čtyř slov, P- Plan (plánuj), D – Do (dělej), C – Check (kontroluj), A – Akt (jednej) [6].

Model PDCA byl připraven především pro efektivní řešení a zlepšování aktivit, procesů a systému. Může být také použit jako jednoduchá metoda pro zavedení změn. Kvalita je obor, kde cyklus zaznamenal hlavní rozvoj a použití v praxi. Model PDCA by měl být součástí znalostí každého poradce, jež pracuje v oblastech systémů kvality, ekologických systémů nebo zajištění bezpečnosti.

Zásady budování a využívání systému řízení bezpečnosti informací (ISMS – Information Security Management System) stanovené výše uvedenými, v české republice platnými normami (tj. ISO/IEC 27001:2005 atd.) se dají interpretovat různými způsoby v závislosti na velikosti organizace. Jejich podstata však zůstává stejná – informační bezpečnost musí být řízena. Velikost organizace a rozsáhlost jejího systému jsou jedním ze základních parametrů při určování způsobu zavádění ISMS. **P**lan, **D**o, **C**heck, **A**ct, tedy Plánování Implementace, Kontrola (sledování) a Vylepšení jsou 4 kroky, které postupně a cyklicky aplikujeme při zavádění a provozu ISMS dle doporučení normy ISO/IEC 27001 v organizaci jakékoliv velikosti. ISMS je možno aplikovat v malé nebo střední společnosti stejně tak jako v nadnárodním gigantu, který zaměstnává i několik tisíc lidí. Interpretace a implementace jednotlivých doporučení se bude diametrálně lišit podle rozsahu systému, počtu pracovních stanic a zaměstnanců tyto obsluhujících, způsobu a hloubce zpracovaní dat a jejich hodnoty apod. Například bezpečnostní politika, jako ten nejvyšší dokument o bezpečnosti informací v organizaci smí obsahovat stejná data jako pro nepoměrně větší společnost. Naopak tomu je u organizace bezpečnosti. Pokud se ISMS zavádí ve větší společnosti, je nutné pro tisíce uživatelů zřídit samostatné bezpečností oddělení s několika lidmi, ve střední firmě na to stačí jeden pracovník a pokud máme systém pro ne více než 10 lidí, tak stačí, když některý ze zaměstnanců bude této problematice věnovat pár hodin ze

své pracovní doby týdně. Podívejme se tedy detailněji, jak vypadají jednotlivé fáze nejpoužívanějšího modelu řízení bezpečnosti IS – PDCA.

2.1.1 Plánuj (Plan)

Tato část by se měla zabývat věcmi týkajících se upřesnění toho, co vlastně od auditu očekáváme, kterým směrem se budeme ubírat a co si vytyčíme za cíl. Řekl bych, že se jedná o část nejdůležitější, je to část, která rozhoduje o krocích budoucích. Je více než zřejmé, že pokud tuto část zanedbáme nebo podceníme, bude nás tato téměř fatální chyba provázet celým implementačním cyklem této metodiky.

2.1.1.1 Plán zabezpečení

Tato problematika je převážně řešena až na úrovni velkých společností, pokud budeme brát v úvahu malé a střední společnosti můžeme konstatovat, že pokud má management zájem a jasnou představu na řešení této problematiky není zapotřebí investovat nemalé prostředky do vypracování této strategie v podobě zadání této práce externí společnosti. Vždy je v prvé řadě nutné určit rozsah a vytyčit přesné cíle, pak jsou výsledky v podobě kvalitní bezpečnostní strategie zaručeny, toto pravidlo platí jak pro malé a střední podniky tak pro velké společnosti, které si tuto strategii nechávají vypracovat nebo mají zvláštní oddělení nebo v některých případech nadnárodních společností i divizi zabývající se touto problematikou v jednom konkrétním podniku.

2.1.1.2 Bezpečnostní politika

Proces tvorby a odsouhlasení „bezpečnostní politiky“ je společný pro všechny typy organizací, taktéž i distribuce této politiky mezi zaměstnance společnosti. Také rozsah a obsah dokumentu je velmi podobný. Bezpečnostní politika definuje zásady a pravidla na úrovni cílů a ty jsou zpravidla shodné pro všechny organizace. Musí také obsahovat odkaz na dokument popisující rozsah ISMS, protože systém řízení bezpečnosti v malé ani střední firmě nemusí být zaveden pro celý informační systém. V dokumentu by měla být popsána mj. organizační struktura bezpečnosti, popis bezpečnostních rolí a jejich odpovědností musí

odpovídat velikosti systému a počtu uživatelů [7]. Navíc je nutné respektovat zavedenou organizační strukturu a proto je možné pro stejně velké společnosti použít různé modely organizace bezpečnosti. Je také třeba určit a rozdělit bezpečnostní odpovědnost. Pokud má systém pouze několik desítek uživatelů, je možné jednotlivé kompetence rozdělit mezi několik stávajících pracovníku z IT, ale není třeba se omezovat pouze na pracovníky z řad zaměstnanců zaměřujících se výhradně na IT problematiku.

2.1.1.3 Rizika - analýza

Konkretizace hrozeb je prvním krokem k vytvoření a správného řízení ISMS. Proto provedení analýzy rizik je nutná nikoli však postačující podmínka pro všechny organizace. Je zapotřebí tuto analýzu provést poctivě protože jenom na tomto základě je možno postavit efektivní výběr a implementaci bezpečnostních opatření. Problematice se věnujeme v následující kapitole.

2.1.1.4 Plán implementace a Prohlášení o aplikovatelnosti

Navazujícím krokem na analýzu a poslední činností v části plánování podle modelu PDCA je vytvoření Plánu implementace a následné Prohlášení o aplikovatelnosti (opatření). Bezpečnostní opatření by měla být vybrána na zvládnutí známých rizik a způsob rozhodnutí se pro jeden konkrétní způsob nezáleží na velikosti podniku. Jejich implementace bude rozdílná, ale například pro všechny organizace lze použít BIS-PD 3005 nebo knihovnu protiopatření CRAMM (vše viz dále) [8]. Velký rozdíl však je ve způsobu a zejména v rychlosti jejich prosazení. Při výběru bezpečnostních opatření je vždy nutné zohlednit jejich dopad na uživatele a na procesy organizace. Je rozdíl změnit proces v malé nebo střední firmě je změna procesu v proces bezpečnější téměř bezproblémová než ve velké společnosti. Plně postačí rozhodnutí ředitele

U velkých společností je velmi pracné obměňovat zavedené postupy. Proto je nutné při výběru protiopatření ve střední firmě více respektovat současný stav. Prohlášení o aplikovatelosti (opatření) je jedním z dokumentu nutných k certifikaci. Obsahuje informace o implementovaných opatřeních normy, případně dalších protiopatřeních navržených na pokrytí rizik. Hlavním cílem je dokumentovat rozhodnutí, pro dané protiopatření bylo či

nebylo vybráno k zavedení. Pokud firma neplánuje být v budoucnosti certifikována, není nutné vytvářet samostatný dokument

2.1.2 Dělej (Do)

Způsob implementace opatření a metody prosazení

Výběr okruhu opatření ISMS je podobný pro malou i středně velkou firmu. Diametrální rozdíl však je ve způsobu a nejvíce v rychlosti jejich prosazení. V menším podniku rozhoduje zpravidla management o tom, kdo bude mít přístup k jakým datům. Ve středním podniku je zapotřebí navrhnout a realizovat proces přidělování uživatelských oprávnění. V malých firmách se rozhodnutí, které zvyšuje bezpečnost ať je složitějšího charakteru, dá realizovat ve velmi krátké době. Následující den může být opatření v systému zcela zavedeno, automaticky používáno a akceptováno. Taková rychlost implementace je typická pouze pro nevelké podniky. Ve středních podnicích je nutné vzít v úvahu akceptovatelnost opatření ze strany uživatelů a další souvislosti jejich realizace. Prosadit například změnu délky hesla vyžaduje revizi směrnice, zapojení několika administrátorů do práce a seznámení desítek uživatelů se změnou, například formou školení. Poté by měla následovat kontrola funkčnosti tohoto protiopatření.

Dokumenty bezpečnosti

Velké rozdíly mezi malým a středně velkým podnikem jsou ve zpracování a míře detailu dokumentace bezpečnosti. Není příliš známo, že uvedené normy striktně nevyžadují papírovou formu dokumentace ani její pevnou strukturu, ale ponechávají na preferencích jednotlivých firem jaká bude forma a obsah zvolena. Přitom právě obava z přehnané formální administrativy je odpuzující pro malé a středně velké podniky od zavádění doporučení těchto norem. Dokumentace ISMS požadovaná k certifikaci podle ISO 27001 musí obsahovat jisté, taxativně uvedené typy dokumentů, dané jednotlivými kroky procesu ISMS, ale jejich rozsah, obsah a forma může být nečekaně jednoduchá a přizpůsobivá. [9]

Zaměstnanci malých podniků se znají a nemalá část bezpečnosti je založena na jejich vzájemné důvěře. Není zapotřebí tvořit složitý systém politik, směrnic a postupů. Je dostačující jednoduché pravidlo, že bezpečnostní dokumentace je vedena ve sdílené složce

elektronické pošty, definovat role a přístupy zodpovědných osob a nezbytné typy bezpečnostních dokumentů realizovat formou elektronických záznamů, obsahující stručný popis realizace daného pravidla, postupu nebo odpovědnosti. Střední podnik se v této oblasti zavedených postupů přibližuje velkému podniku. V tomto případě je zapotřebí zavádět detailnější administrativní procedury, protože existuje více oddělených rolí a odpovědností a také více definovaných pravidel. Tato administrativa je nutná, aby byly potlačeny všechny úkony, které se dějí při práci s daty jen tak, na „dobré slovo“. Rozsah a aktuálnost bezpečnostní dokumentace bývá velmi často jedním z hlavních kritérií při posuzování kvality ISMS a míry dosažené shody s požadavky norem.

Program zvyšování bezpečnostního povědomí

Mezi další metody prosazení bezpečnostních pravidel v organizacích je zařazen program zvyšování bezpečnostního povědomí v organizacích. Tato jednoduchá, levná a velice účinná metoda bývá bohužel mnohdy v malých a středních podnicích opomíjena. A právě zaměstnanci, kteří jsou nezřídka zdrojem bezpečnostních incidentů a kteří mohou, pokud jsou kvalitně informováni, svým včasným jednáním šíření a škodám incidentu předcházet. Pořád se můžeme setkat s nepochopením, když zdůrazňujeme, že nejvyšší hodnotu pro organizaci mají v informačním systému data a nikoliv hardware a software. Existuje stále také mnoho uživatelů, kteří pokládají svou disketu nebo lokální harddisk „svého počítače“ v zaměstnání za mnohem bezpečnější uložiště, než síťový disk s transparentně nastavenými přístupovými právy a pravidelným zálohováním. A přitom bohatě postačí, pokud zvyšování bezpečnostního povědomí opřeme o stručné vstupní školení všech zaměstnanců a občasné prodiskutování aktuálních bezpečnostních otázek dle potřeb organizace a vývoje nových potencionálních hrozeb. U velkých podniků zavedeme pravidelná školení či bezpečnostní přednášky například ve spojení se stmelováním pracovních týmů. U velkých podniků by také nemělo být zapomínáno na fakt, informovat všechny zaměstnance dle potřeby o aktuálních hrozbách a opatřeních, např. formou zřízení centrálního informačního místa o bezpečnostních otázkách na firemním intranetu.

Způsob zvládání rizik za provozu

Jedním z nejpodstatnějších příčin zavádění ISMS, je potřeba zajistit kontinuální proces zvládání a řízení informačních rizik. Základem jejich zdárného řízení je identifikace a analýza všech potencionálních rizik a následné rozhodnutí o způsobu jejich zvládání a sledování v čase. Účelem řízení rizik není veškerá identifikovaná rizika bezezbytku pokrýt, ale pokrýt zvolenými opatřeními pouze taková, u kterých je to účelné. Ostatní rizika může organizace akceptovat a monitorovat, další může delegovat na jiný podnik, popřípadě je pojistit. Pouze pokud organizace zná a monitoruje všechna rizika související s ochranou informací a příslušně rozhoduje o způsobu jejich zvládání, potom smí prohlásit, že tyto rizika jsou pod kontrolou. Tyto zásady jsou opět společné pro všechny velikosti a typy podniků.

Nároky na provoz opatření a zajištění bezpečnosti

Součástí strategie zvládání rizik je i monitorování nároků na provoz jednotlivých opatření a celkového zajištění bezpečnosti. Zatímco u malých podniků není zapotřebí plánovat ani vyhrazovat samostatný rozpočet, neboť eventuelní nákup a provoz nezbytných opatření je v případě okamžité potřeby schválen managementem a hrazen dle aktuálních potřeb podniku, u středních a velkých podniků je nezbytné realizovat alespoň rámcové plánování nutných peněžních i lidských zdrojů. Z hlediska preferencí při výběru prevence hrají celkové nároky na jejich zavedení a provoz hlavní roli. Zatímco pro malé podniky není překážkou flexibilně implementovat administrativní a personální opatření i za cenu vyšších požadavků na pracovní sílu, kamenem úrazu však bývají finanční náklady na pořízení složitých technologických opatření. U velkých podniků lze tyto preference vysledovat obráceně, protože pro ně bývá jednodušší flexibilně zavést nové technologické opatření, než jej nahradit administrativními či organizačními změnami. V případě preferencí středně velkých podniků je stav logicky někde uprostřed. Záleží na flexibilitě řízení, technologické úrovni a znalostech zaměstnanců podniku, k jakým typům opatření se budou inklinovat více.

Implementace opatření DRP a IRH

Poslední neméně důležitou oblastí opatření při implementaci a provozu ISMS je tvorba a údržba Havarijních plánu (DRP – Disaster Recovery Planning) a Postupu řešení bezpečnostních incidentů (IRH – Incident Response Handling). Obdobně jako v případě ostatních formálních postupů i zde platí, že pro malé podniky je neefektivní vypracovávat a udržovat podrobné formální havarijní plány.

Pro obnovu systému jim plně postačí tvorba rámcového univerzálního havarijního *checklistu* pro všechny možné situace havárie, který bude obsahovat postup bezpečného vypnutí a restartu technického vybavení a serveru, jednoduchý záznam výsledné konfigurace technologií a aplikací, postup obnovení dat ze záložních médií a seznam kontaktů na interní a externí osoby, které mohou být užiteční při výskytu havárie nebo závažného bezpečnostního incidentu. Tyto havarijní postupy by měly být alespoň základně testovány a potom jen při zásadní změně používaných technologií a služeb. U středně velkých podniků je silně doporučeno rozšířit havarijní *checklist* i o popis kroku instalace jednotlivých segmentů IS a obnovy dat a aplikací ze záloh. U složitějších IS je zapotřebí rozlišit obnovu strategických aktiv od méně strategických a tomu podřídit priority v havarijním plánování. Pro výběr strategie způsobu obnovy a nastavení priorit je nejlépe realizovat analýzu dopadu na činnosti organizace (BIA – Business Impact Analysis). Pokud byla kvalitně realizována analýza rizik, lze informace o negativních dopadech nedostupnosti jednotlivých aktiv nalézt tam. Na základě těchto výsledků je vyhotoven strukturovaný havarijní plán obnovy, obsahující možnosti postupu dle specifikovaných typů havarijních stavu. Takovýto plán je nutné periodicky testovat a aktualizovat a na základě výsledku testu (v porovnání s cíly obnovy) zefektivňovat. [10]

2.1.3 Kontroluj (Check)

Sledování provozu

Sledování provozu zásadních částí informačního systému a ochranných procedur je základním zdrojem informací pro kontrolu jejich funkčnosti a spolehlivosti. Pokud podnik realizující ISMS plánuje v budoucnu i jeho certifikaci uznávanou autoritou, musí vytvářet a kumulovat záznamy o fungování alespoň těch opatření, která jsou uvedena v Prohlášení o aplikovatelnosti (ty budou předmětem auditu). Ale ne všechny typy opatření samy automaticky generují záznamy o činnosti a tak je nezbytné přistoupit i v prostředí malých a středních podniků k nepříliš populárnímu manuálnímu generování záznamu u takových opatření, která tuto vlastnost nemají (především organizační a administrativní). Není pravidlem, že se musí jednat o únavnou administrativu, protože rozsah a složitost opatření,

zvláště u malých a středních podniků, nebývá nijak zásadní. Příkladem toho, co je dostačující pro audit funkčnosti opatření „bezpečnostní školení uživatelů IS“, jsou seznamy účastníků školení, datum a předmět školení. Povinnost vůči případnému auditu ISMS a certifikaci je splněna. Pro sledování ICT je postačující u malých podniků výchozí nastavení logování dle standardní instalace většiny produktů a jejich manuální náhodná kontrola zodpovědným pracovníkem.

U středních podniků, je již vzhledem ke složitosti IS infrastruktury nepostačující spoléhat pouze na náhodné manuální kontroly logovacího souboru a je nutné použít automatických nástrojů pro jejich filtrování a vyhodnocování nestandardních událostí např. pomocí skriptů nebo obdobných produktů. [11]

Testování funkčnosti opatření

Pasivní metody kontroly je zapotřebí doplnit i o aktivní a preventivní způsoby, jako např. aplikační kontroly chyb výpočtu a zpracování dat nebo testování zranitelností, popřípadě penetrační testování systému. Zatímco komplikovanější a časově i finančně náročnější penetrační testování má za cíl napodobení reálného útoku z vybraného prostředí a identifikaci možných negativních dopadů na IS, bezesporu jednodušším, rychlejším a levnějším způsobem testování odolnosti vůči útokům je vyhledání a testování zranitelností provozovaných ICT produktů. Všechny tyto způsoby mohou být realizovány z vnitřní sítě, nebo častěji z externího prostředí – z většiny případů z Internetu, což by měly být v případě malých a středních podniků hlavní oblasti prevence proti útokům na IS. Protože se v případě penetračního testování jedná o vysoce specifický úkon, vyžadující detailní znalosti o technikách a nástrojích hackingu, obdobně jako o bezpečnostních slabinách jednotlivých ICT produktů a komunikačních protokolů, je tento úkol určen specializovaným externím firmám, které disponují dostatečným profesním zázemím pro jejich kvalifikovanou realizaci. Naproti tomu testování zranitelností je proces, který si mnohdy mohou počítačově zruční uživatelé provést sami, pomocí volně dostupných programů nebo využít specializovaných webových služeb. Pro střední a velké podniky by testování zranitelností klíčových serverů a služeb IS mělo být rutinní záležitostí, alespoň po implementaci bezpečnostních opatření a před běžným provozem komunikačních spojů. Pokud střední a velké organizace provozují citlivá data a aplikace na Internetu, mohou zvážit realizaci penetračního testování nebo podrobný technický bezpečnostní audit konfigurace klíčových prvků IS a bezpečnostních

zásad jako např. Firewallu, DNS nebo Internetového aplikačního nebo databázového serveru či routeru na rozhraní LAN/WAN. [12]

Audit a kontrola bezpečnostních opatření

Spolu se sledováním provozu, testováním zranitelností a technicky zaměřeným auditem konfigurace ICT, je další metodou kontroly implementace a provozu IS/ISMS realizace Auditu a kontrol bezpečnosti IS. V zásadě lze říci, že audit opatření musí být prováděn v každém typu a velikosti podniku, která provozuje systém řízení nad opatřeními, jinak by neexistovala zpětná vazba o stavu reality vůči plánu a návrhu požadovaného cílového stavu. V případě ISMS by měl audit obsahovat kontrolu funkčních bezpečnostních i direktivních opatření ISMS, která jsou deklarována v Prohlášení o aplikovatelnosti a popsána v bezpečnostní dokumentaci. Audit by měl provést zhodnocení, jak jsou realizována v praxi. U malých podniků není zapotřebí tvořit samostatná pracoviště nebo pracovní zařazení interního auditora, ale je zapotřebí i v malém podniku funkci interního auditora dedikovat, alespoň jako částečný pracovní úvazek některého zaměstnance nejlépe IT oddělení. Jednou za rok je nezbytné projednání zjištěných výsledku plánovaných auditu i občasných kontrol s managementem podniku a potom i se všemi zaměstnanci. V případě středně velkého podniku se je již záhodno zvážit vytvoření samostatné funkce interního auditora, kterému připadne i funkce bezpečnostního auditora. I v tomto případě má za úkol provádění plánovaných i náhodných kontrol dle ročního i operativního plánu auditu, který je konstruován s přihlédnutím k nejvážnějším rizikům a nálezům minulých auditů. Pro dosažení vyšší odborné úrovně a komplexnosti výsledku kontroly je doporučováno uskutečnit nejméně jedenkrát za rok přehledový porovnávací audit stavu ISMS, vzhledem k požadavkům norem ISO, s participací alespoň jednoho externího odborného konzultanta.

Revize adekvátnosti a efektivnosti ISMS

Kromě ověření funkčnosti, spolehlivosti a komplexnosti funkčních i řídících opatření je třeba přibližně jednou za rok zrevidovat rozsah, adekvátnost a efektivnost celého ISMS ve vztahu k potřebám, cílům a prostředí organizace. Výsledek této celkové revize ISMS by měl být stejně jako souhrnné výsledky auditu opatření projednán s vedením organizace a pořízeny záznamy o přijatých opatřeních. Protože se jedná o činnost vyžadující široký

přehled a komplexní zkušenosti z oblasti bezpečnosti informací a implementace ISMS v podnicích, musejí se malé i střední podniky spolehnout na pomoc externích autorit, stejně jako v případě analýzy informačních rizik v etapě PLÁN.

2.1.4 Jednej (akt)

Vyhodnocení fáze CHECK

Elementárním předpokladem pro vhodné rozhodnutí „co a jak dál“ by vždy měly být co nejkonkrétnější a nejkomplexnější informace o aktuálním stavu a cílech organizace. Informace o momentálním stavu týkající se sledování provozu, evidence chyb a bezpečnostních incidentů, výsledků testování funkčnosti a spolehlivosti implementovaných opatření, výsledků testování zranitelností a výsledky interních i externích auditů poskytuje předcházející fáze „Kontroluj“. Vyhodnocení těchto informací provádí v malých podnicích zaměstnanec delegovaný činností bezpečnostního manažera. Výsledky svého zjištění by měl nejméně jedenkrát za rok předložit majiteli, případně managementu podniku a společně provést jejich analýzu a vyhodnocení. U středních a velkých organizací se již vyplatí přidat do tohoto kroku také revizi návrhu a možných zefektivnění bezpečnosti informací i procesu ISMS, jejichž evidenci zastřešuje fórum pro bezpečnost informací, složené ze zástupců uživatelů, dodavatelů a odborných rolí delegovaných pro oblast bezpečnosti informací v organizaci. V rámci procesu řízení rizik je realizováno také periodické přehodnocování úrovně zbytkových a přenesených rizik, s ohledem na změny v organizaci, technologiích, podnikatelských cílech a vnějších událostech a hrozbách.

Identifikace a analýza neshod

I když byla revize výstupů auditu zahrnuta již do předchozího kroku, je více než vhodné tuto činnost rozepsat detailněji. Identifikace a analýza neshod má za úkol rozebrat výsledky interního i případného externího auditu a posoudit, které z nalezených neshod jsou skutečné, které pouze potenciální a eliminovat špatně identifikované neshody. Toto rozhodnutí je opět vhodné zaevidovat formou tabulky. Nakonec je pro odstranění skutečně identifikovaných neshod třeba navrhnout nápravná opatření a pro zabránění opakovaného

výskytu skutečných i potencionálních neshod v budoucnu je třeba navrhnout preventivní opatření. Jejich výběr, implementace a ověření funkčnosti je již náplní dalších paralelních PDCA procesu (koleček), které jsou realizovány pro každé další navržené opatření. U malých podniků provede tuto analýzu neshod majitel, případně management organizace, ve spolupráci s pracovníkem pověřeným funkcí bezpečnostního manažera. S výsledným rozhodnutím je vhodné seznámit všechny uživatele. Implementace těchto rozhodnutí bývá velmi rychlá a flexibilní. Pokud menší podnik usiluje o certifikaci ISMS, je vhodné obrátit se pro pomoc na externího konzultanta, případně zrealizovat srovnávací audit procesu ISMS vzhledem k ISO 27001 externí specializovanou firmou a s její pomocí navrhnout potřebná nápravná opatření pro dosažení souladu. U středních podniků bude interpretace výsledku auditu i návrh nápravných a preventivních opatření komplikovanější a formální proces, řízený pracovníky interního auditu ve spolupráci s dalšími zainteresovanými odbornými pracovníky organizace. Při přípravě na certifikaci ISMS se i zde doporučuje sáhnout pro pomoc externích odborníků, pokud takoví nejsou ve vlastních řadách.

Nápravná a preventivní opatření

Nápravná opatření slouží k odstranění skutečně nalezených nedostatků a chyb, spojených se zaváděním a provozem ISMS a k zabránění jejich dalšímu trvání (opakování). Jedná se například o částečnou implementaci opatření zvolených v Prohlášení o aplikovatelnosti opatření, o chybějící dokumentaci těchto opatření, o nedostatečné proškolení pracovníků podílejících se na procesu ISMS apod. Preventivní opatření jsou vybírána s cílem zamezit výskytu potencionálních neshod v budoucnu, tedy za účelem minimalizace příčin, které by mohly vést ke vzniku reálné nežádoucí situace a reálné neshody. Příkladem takové potencionální neshody může být například nedodržení oddělení rolí u některých činností a opatření ISMS nebo nedbalé provádění nutných monitorovacích a kontrolních činností. Pro malé podniky je typická rychlá praktická změna bez byrokratických průtahů a příklon především k organizačním a personálním opatřením, jejichž „pořízení a zavedení“ bývá pro majitele malých firem nejpřijatelnější. Pro střední podniky, stejně jako ve fázi DO (popis nároku na provoz opatření), není již hledisko nákladu na pořízení a zavedení opatření tak palčivé jako pro malé podniky a bude při jejich výběru více rozhodovat jeho účinnost a pokrytí nalezených nedostatků.

II. PRAKTICKÁ ČÁST

3 IMPLEMENTACE VE VYBRANÉ SPOLEČNOSTI

3.1 Plán projektu

S přihlédnutím k výše popsaným normám a legislativě bychom mohli nabýt dojmu, že provedení Bezpečnostního auditu v konkrétním podniku je rutinní vyplňování předem nadepsaných konkrétních úkonů nebo odškrtáváním v již napsaném seznamu. Není tomu tak. Každý podnik je svým způsobem originál a má své specifické požadavky a potřeby. Není na místě se přesně držet norem, protože se může stát, že provedený audit bude spíše kontraproduktivní soubor pravidel než jakýsi doklad toho, že data uložená v našem podniku jsou chráněna před zneužitím. V případě společnosti poskytující služby IT, jsme řešili předem přesně definované úkoly a výsledky prezentovali v předem dané formě výstupu. Nebylo záměrem, aby společnost dosáhla certifikace od některé z akreditovaných společností, nicméně některé postupy a doporučení z norem pro audit vycházejí. Cílem auditu bylo poskytnout podniku soubor pravidel zaručujících bezpečnost dat zákazníků v co možná nejvyšší míře.

3.2 Definice projektu

Ze strany zadavatele – *podniku poskytujícího služby IT* byly určeny úkoly, které má bezpečnostní audit řešit, stejně tak i forma výstupu ke každému úkolu. Bylo třeba řešit následující:

1. **Analýza a základní přehled o stavu ICT**

   Architektura ITC, LAN/WAN sítě, servery/OS/aplikace, pracovní stanice, zhodnocení zálohovací strategie.

   Výstup: Přehled a popis řešení ICT ve společnosti

2. **Zhodnocení míry bezpečnosti**

Ochrana počítačové sítě před útoky z internetu a z lokální sítě; zhodnocení bezpečnosti vzdálených přístupů do sítě auditovaného podniku; zhodnocení bezpečnosti a perspektivy používaných a možných typů komunikačních připojení k serverům a aplikacím z hlediska ochrany dat.

Výstup: Zpráva obsahující veškeré zjištěné nedostatky v rámci konfigurace sítě, jejích bezpečnostních prvků a dalších komponent + doporučení ke zjednání nápravy a k implementaci změn včetně dopadu do interních procesů a směrnic.

3.3 Základní přehled stavu ICT

3.3.1 Aktuální konfigurace a nastavení zabezpečení

Během hodnocení byla ověřena aktuální konfigurace bezpečnosti v doménovém prostředí podniku. Základem bezpečnosti je použití standardních mechanismů v Active Directory. Součástí hodnocení byla doména založena na serverech W2003. Domain a forest functionality level je nastavena na W2003 native.

Zjištěné domény viditelné přes protokol NETBIOS ze stanice v doméně Windows 2003:

- popron1.local – samostatná doména W2003
- popron.cz – doména pro zdroje dostupné z internetu

Stávající konfigurace domény, síťový model a způsob použití IT neselektuje provozní prostředí pro pobočku Ostrava a pobočku Praha. Z pohledu IT je vše navrženo tak, jako by šlo o jeden právní subjekt. Proto bude v dalším textu uvedeno hodnocení celého prostředí pro pobočku v Praze, které bude stejné jako pro pobočku v Ostravě. Doména Windows 2003 pod názvem popron1.local nemá zřízen defaultní obousměrný tranzitivní trust do dalších domén. Politika hesel je v současnosti nastavena pro doménu W2003 následovně:

- Minimální délka hesla: 6 znaků
- Maximální stáří hesla: 42 dnů

- Minimální stáří hesla: 0 dnů
- Zamykání účtů: nenastaveno
- Historie hesel: 24 passwords

Tato politika je z pohledu bezpečnosti nedostatečná a musí být zpřísněna. Není používáno např. automatické uzamykání uživatelských účtů po 5 neúspěšných přihlašovacích pokusech. Rovněž délka hesla by měla být delší – alespoň 7 znaků pro běžné uživatele a 10 znaků pro administrátorské účty. Délka hesla je klíčová pro zajištění bezpečnosti domény W2008/W2003. Heslo délky 6 znaků může být dešifrováno na běžném PC v řádu desítek hodin. Běžný uživatel v doméně Windows 2003 má přiděleno login jméno tvořené 5 znaky uživatelova příjmení a prvními dvěma písmeny ze jména. Případné duplicity login jména jsou řešeny přidáním číslice 2. Uživatelé často používají doménové heslo i do systému pošty a dalších aplikací. Proto doporučujeme použít shodnou politiku pro práci s hesly na všech systémech. Nová politika by měla vynucovat heslo alespoň 7 znaků dlouhé s pravidelným měněním každých 42 - 90 dnů. Je zapnuta tzv. komplexita hesel ve W2003 doméně. Měla by se nastavit politika blokování uživatelského účtu na 30 minut po 5 neúspěšných pokusech o přihlášení. Tato politika se musí před nasazením důkladně odladit v testovacím prostředí.

Uživatel je zaváděn do IS správcem podle požadavku personálního oddělení zadáním do databáze Helios Green IS. Z těchto databází jsou synchronizovány informace o aktuálních uživatelích do dalších databází a aplikací pomocí specializované aplikace. Tato aplikace se startuje jako služba každých 10 minut. Synchronizace pro konfiguraci karet na vstupní vchodové dveře probíhá pouze 1x denně ve 3:00. Vedoucí pracovník daného oddělení definuje požadavky na aplikace, ke kterým má mít daný uživatel přístup. Uživatel nestvrzuje svým podpisem seznámení se zásadami práce a bezpečnosti IT. Správce vytvoří účet v Active Directory a email účet v systému Exchange. Při odchodu zaměstnance je jeho účet vypnut v AD.

3.3.2 Charakteristika prostředí koncových PC

Klient PC slouží jako prostředek pro práci s aplikacemi typu Office a zajištění přístupu ke kritickým aplikacím Helios Green IS. Organizace dále používá cca 30 přenosných počítačů. Klíčové aplikace běží na uživatelských stanicích s operačním systémem Windows XP Professional se SP 2 a 3, kde je zpracovávána běžná kancelářská činnost v produktech MS Office a klíčových aplikacích. K dispozici je přístup na terminál server pomocí klientů od firmy Microsoft. Uživatelé mají přístup jenom k aplikacím a jejím částem na základě principu „nutná potřeba k práci“. Činnost uživatelů je omezena uživatelskými profily a jejich přístup k autorizovaným službám a aplikacím je kontrolována správci aplikací při zavádění do systému a aplikační logikou. Jsou provozovány následující hlavní aplikace:

- MS Office, Adobe Reader
- Sada Office – Microsoft
- SQL server - Microsof
- Pošta MS Outlook,
- WWW prohlížeč MS Explorer a Mozilla
- Aplikace pro styk s bankou – Profibanka, Gemini a další
- Aplikace Helios Green IS – informační systém.
- Antivir AVG a MS Forefront, Adware AntiSpyware klient.

Všechny zjištěné aplikace byly pokryty řádnou licencí. Tyto aplikace a práva v nich jsou přidělovány uživatelům podle potřeby dle organizační struktury. Zálohování databází se provádí denně ve večerních hodinách naplánováním automatického spouštění služby exportu dat v plánovači Windows. Uživatelé ponechávají data na klientovi. Antivirový sw je používán na klientech a denně se ověřují nové aktualizace z Internetu. Vzdálené přístupy jsou řešeny pomocí Kerio VPN klienta a jsou určeny pouze vybraným skupinám uživatelů. Správce nemá oficiálně k dispozici druhý antivirový a antispyware software. Kontrola přístupu na WWW stránky není aplikována a nefiltruje např. www.freefoto.cz a www.porn.com. V době hodnocení byly tyto stránky bez problémů přístupné.

Uživatelé si uvědomují potřebu chránit některé informace a uvítali by bezpečnostní mechanismy, které zajistí adekvátní ochranu. Pro definované množiny informací existuje definovaný vlastník (zpravidla správce aplikace), který rozhoduje o přístupu jednotlivých

uživatelů ke zdrojům aplikace. Na sdílené adresáře mají standardně přístup všichni členové dané studijní skupiny. Existují speciální adresáře, kde je zřizován přístup podle potřeby. Definici těchto přístupů dělá správce podle principu „nutná potřeba znát ke své práci“.

V této společnosti existuje relativně malé právní povědomí o bezpečnosti IT mezi uživateli. Uživatelé požadují zajistit ochranu některých skupin dat, které potřebují ke své práci a jsou ochotni používat bezpečnostní technologie i když to omezí jejich práci. Přehled dat vyžadujících ochranu je v následujícím seznamu:

1. Finanční data – účetnictví, styk s bankou,
2. Personální informace – informace o zaměstnancích organizace,
3. Obchodní informace – seznam dodavatelů, nákupní ceny atd.,
4. Informace o infrastruktuře IT – rozsahy IP adres, schéma zapojení atd.

Uvedený seznam je pouze orientační a může být doplněn podle potřeby. Většina uvedených informací je určena pouze pro omezenou skupinu vlastníků. U některých informací je třeba řešit rychlé zastarávání v čase.

Uživatelé ke své činnosti potřebují jenom minimum externích médií a není třeba řešit centrální ukládání dat na externích médiích. Uživatelé můžou ukládat data na USB flash disky. Tento přístup může správce ovlivnit v registrech. Antivirová ochrana je zajištěna pomocí programu AVG nebo MS Forefront na běžících stanicích, AVG bez centrální správy. V současnosti je místo nástroje AVG nasazován Forefront Client Security s centrální správou. Na Exchange serveru se používá Forefront for Exchange, na firewallu Kerio se používá eTrust Antivirus, kontrolující HTTP, SMTP, FTP a POP3 komunikaci. Podpora Keria pro e-Trust antivirus bude v brzké době ukončena, proto je pro firewall potřeba včas pořídit jiný antivirový program. Tiskové služby jsou zajištěny na síťových tiskárnách přes tiskové servery (např. HP JetDirect).

3.3.3 Fyzická bezpečnost místnosti serverů

Bezpečnost serverovny je zajištěna kamerovým dohledem s automatickým odesláním SMS při pohybu v serverovně. V budovách je používána kontrola vstupu na karty a dohledem na

vrátnici v každé budově. Do budov existuje hlavní vchod hlídaný vrátným a dva pomocné vchody ze dvora, které slouží i jako únikové východy. Místnost serverů je dislokována v hlavní budově v prvním patře. Vstup je povolen pro cca 3 zaměstnanecké role a vrátné, kteří mají přístup v mimopracovní dobu. Na vrátnici je umístěn klíč pro otevření serverovny v případě nouzové situace. V obou budovách je v přízemí použita kontrola pohybu osob pomocí snímačů EZS. Ve vyšších patrech jsou snímače pouze na chodbách a v místnosti serverů. Hlášení je vyvedeno na pult centrální ochrany u externí firmy.

Automatické hašení požáru není v místnosti serverů použito. Za dveřmi je umístěn samostatný hasební přístroj. Nepoužívají se snímače požáru, ale je detekována teplota a vlhkost. Jeden snímač pohybu je připojen na centrální dohled pro celou budovu. Snímač EZS je rovněž na vstupní chodbě před místnosti serverů. Přístupová chodba není vybavena nouzovým osvětlením. V místnosti serverů nejsou vyzděné a utěsněné všechny průduchy a prostupy. Je nutné vyplnit prostupy nehořlavou hmotou např. od firmy Hilti. Není označena veškerá kabeláž v rozvaděčích. Chybí emergency tlačítko vypínající přívod elektřiny v celé místnosti. Vstupní zámek je jednoduchý bez ochranných prvků. Vnější stěny místnosti jsou s dostatečnou tloušťkou. V současnosti jsou všechny servery umístěny volně na stole a nejsou v rozvaděčích. Místnost serverovny lze považovat za bezobslužné pracoviště s požadovanou kontrolou přístupu. Všechny servery jsou připojeny na centrální UPS – MGE Pulsar. Ta garantuje napájení po dobu cca. 40 minut. Po 30 minutách napájení z baterií dojde k automatickému vypínání připojených serverů. Napájení je dvouokruhové se samostatným jištěním. V minulosti nebyly zaznamenány dlouhodobé výpadky napájení – pouze v minutách cca 1x ročně. Počítače uživatelů se standardně nepřipojují k dedikovaným napájecím rozvodům zálohovaných na UPS. Serverovna nemá protipožární dveře s plnou výztuží. Dveře nejsou chráněny proti vysazení z pantů. Kabeláž procházející přes stěny není vytmelena pěnící hmotou a snižuje se tak odolnost proti požáru. Všechny komponenty v místnosti serverů jsou chlazeny klimatizací ze stropu. Použitá klimatizace je KIMO 12 PW - ON / OFF EKONOMICKÁ TŘÍDA A+A a dodala ji a údržbu provádí Climatex, s.r.o. Praha. Klimatizační jednotka je umístěna u stropu a zajišťuje náporové chlazení. Během revize byla po vypnutí klimatizace naměřena teplota v místnosti 23 stupňů. Na klimatizační jednotce byla nastavena chladící teplota 23 stupňů. Test klimatizace musí být prováděn před začátkem letních měsíců. Definovaní pracovníci pravidelně provádějí údržbu klimatizace a UPS.

Protipožární ochrana je řešena na úrovni celého komplexu budov. Místnost serverů tvoří samostatný požární úsek se zvýšenou protipožární odolností. Jsou zajištěny jednotlivé požární úseky. Všechna provedená opatření jsou nastavena dle požadavků platné legislativy na ochranu lidských životů. Bohužel nejsou zohledněny požadavky na ochranu IT komponent. V případě většího hasičského zásahu v chodbě nebo vyšších patrech by došlo ke zničení všech klíčových IT komponent umístěných v serverovně a to např. průsakem hasící vody, vodní parou vzniklou během zásahu nebo kouřem z požáru atd. Toto riziko je vzhledem k umisťování záloh mezi lokalitami akceptovatelné.

3.3.4 Organizační bezpečnost a zálohování

Pro chod IT komponent je klíčové rozdělení odpovědnosti za jednotlivé činnosti. Správcovské procesy nejsou rozděleny mezi dostatečný počet pracovníků. Klíčová je osoba správce, který může vykonávat potenciálně nebezpečné činnosti a má neomezené pravomoci. Použité technologie neumožňují plně eliminovat chybnou činnost správce. Částečně může být použito šifrování pro ochranu dat, ale tyto technologie sebou nesou další technické problémy v případě nutnosti obnovit zašifrovaná data. Bez přímé podpory IT se organizace obejde minimálně 24 hodin do následujícího pracovního dne. Po této době musí být k dispozici alespoň omezené zdroje zajišťující minimální funkce IT s konektivitou do Internetu.

Pro zálohování se používá nástroj MS Data Protection Manager. Zálohování se provádí na externí datové pole nespecifikovaného výrobce s kapacitou 3TB. Standardně se data udržují na diskovém poli připojeném k záložnímu serveru. Toto diskové pole používá technologii zajištění dat RAID5 a k dispozici má jeden hot spare disk. Celková kapacita je rovněž 3TB. Server má zrcadlený disk c: a data jsou na disku d:, který je rovněž typu RAID5 + hot-spare. K dispozici je jeden disk pro ukládání dat pomocí technologie shadow copies. Tato technologie zajišťuje zálohování čerstvých dat pořízených během daného dne. Není tedy nutno vždy obnovovat poslední data ze záloh. V některých případech jde obnovit konkrétní kopie souborů a adresářů z disku s obsahem shadow copies. Během auditu docházelo ke změně zálohovacího nástroje a nebyl k dispozici kompletní plán zálohování a obnovy dat. Zálohování probíhá po síti na síťové úložiště, takže data odchází z místnosti pořízení.

3.3.5 Charakteristika práce na koncových PC

Na uživatelských PC probíhá většina každodenních činností prováděných uživateli v rámci běžné pracovní činnosti. Klienti používají operační systém Windows XP se SP2 a SP3. Uživatelé nemají za povinnost ukládat všechna data na server a ponechávají některá data na klientech. Data uživatelů se synchronizují, publikují a sdílejí přes sdílené adresáře. Servery popron1, popron2 slouží jako centrální servery určené pro běh klíčových aplikací. Další terminal server slouží pro obsluhu tenkých klientů Fujitsu-Siemens Futuro A220 a pro vzdálené připojování uživatelů.

Uživatelé nepoužívají screensaver, který by po několika minutách zamknul uživatelský počítač. Uživatelé nevědí, že se musí odhlašovat ze systému nebo si zamykat počítač při opuštění pracoviště. Uživatelé jsou nuceni používat politiku hesel - 6 -14 znaků. Uživatelé připouštějí, že mají v hesle uvedeno např. jméno rodinného příslušníka atd. Po 5 chybných pokusech o přihlášení nedochází k uzamčení účtu. Obdobně nedochází k zamykání účtu v aplikacích. V rámci historie hesel systém Windows 2003 vynucuje neopakovatelnost posledních 25 hesel.

Na počítačích se používá rezidentní antivirová ochrana AVG. Prostředí antiviru není spravováno z centrální konzoly. Uživatelé zpravidla nespouštějí antivir a spoléhají se na rezidentní štít. Většina PC není umístěna v místnostech s EPS a nepoužívá se kontrola přístupu na kartu do místností. Omezeně je aplikováno pouze uzamykání místností a vstup do budov na kartu.

Uživatelé ponechávají data na svých pracovních stanicích a přenosných počítačích. Sdílená data pro všechny jsou dostupná na disku S:. Data dostupná pro všechny členy stejné skupiny jsou na disku K:. Personální data má každý uživatel na disku O:. Předávání dat mezi učiteli a správci probíhá přes disk U:.

Záleží na uživatelích, jak často si synchronizují data na přenosných počítačích a pracovních stanicích. Na přenosných počítačích se nezadává heslo do BIOSu pro přístup k disku a nepoužívá se funkce HardDrive Lock pro šifrování disku na úrovni diskových ovladačů. Tímto mechanismem nejsou data šifrována ani na serverech.

3.3.6 Zjištěné klady

Bezpečnost celého prostředí společnosti se opírá o bezpečnostní mechanismy v doméně Windows 2003. V této doméně byly začleněny během auditu všechny pracovní stanice. Používají se tencí klienti od firmy NCoputing a 40 tenkých klientů od Fujitsu-Siemens, což garantuje shodné bezpečnostní nastavení pro všechny tyto klienty. I když nejsou využity všechny bezpečnostní mechanismy, poskytuje doména W2003 dostatečný základ pro vynucení potřebných bezpečnostních zásad. Je zaveden centralizovaný model bezpečnosti PC na úrovni jediné domény Windows 2003 a pomocí technologie GPO jde provádět management stanic začleněných v doméně. Mechanismus GPO je použit shodně na všechny subjekty. Používá se omezení a konfigurace uživatelských stanic pomocí Group Policy (GPO) a během revize byla na klientech aplikována kromě standardní domain politiky také omezení pro firewall, přesměrování dokumentů, automatické nastavení záplatování pomocí služby WSUS atd.. Celkový přehled je uveden v následujících seznamech.

Na počítače se aplikují následující GPO politiky:

- Default domain policy
- Confmngr2007
- WMP - ne úvodní okna

Na uživatelské účty se aplikují následující GPO politiky:

- Default Domain Policy
- Kerio odhlašovací script
- Přesměrování dokumentů na O:
- IE 7

Neexistuje přímá konektivita do jiných sítí kromě definovaných bodů, zajišťujících VPN přístup a konektivitu na Internet. Nepoužívají se WiFi sítě. Prvky sítě a jejich konfigurace jsou pod trvalou kontrolou správce a externího dodavatele. Lokalita Praha má dostatečnou síťovou konektivitu, ale nemá záložní spoje na Internet přes jiné fyzické linky. V budoucnu je třeba zvážit posílení přenosového pásma na Internet. Všichni klienti a servery používají shodné informace o dané subsíti zejména: DNS a DG. Testování internetového připojení proběhlo bez zjištění závažných nedostatků vedoucích k průniku. Na všechny klienty a servery je v současnosti použita politika automatického aplikování bezpečnostních záplat.

Automaticky jsou instalovány všechny kritické záplaty. Před ukončením bezpečnostní revize byla provedena závěrečná kontrola chybějících updatů. Kontrola potvrdila správnou činnost automatického záplatování pomocí komponenty WSUS. Instalace nových Service packů probíhá manuálně po kontrole správcem. Veškerá IT aktiva jsou rozmístěna v budově, která je pojištěna proti krádeži a zničení aktiv.

3.3.7 Zjištěné nedostatky

Během hodnocení byly nalezeny nedostatky s různým stupněm kritičnosti. Je třeba odstranit následující nedostatky:

- Na všech klientech s Windows XP běží standardně služba SSDP (port 1900/UDP), která může být zneužita k získání přístupu na klienta. Tato služba musí být vypnuta. Podrobnější info je na: http://www.updatexp.com/upnp_security.html. Hrozba je snížena použitím správného hotfixu na všech stanicích, přesto doporučujeme tuto službu vypnout.
- Na klientech a serverech je nastaveno cachování přihlašovacích informací – Cached Logon Credentials. V praxi tak může legální uživatel získat heslo administrátora, který se přihlásil alespoň 1x na stanici např. po technickém zásahu. Standardně je klíč HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount nastaven na default hodnotu 10. Tuto hodnotu je třeba změnit na 0 (úplné vypnutí cachování na stanicích v LAN, uživatel se nepřihlásí bez DC) nebo na 1 – pouze poslední uživatel pro přenosné počítače.
- Na klientech není zapnut bezpečnostní audit, kromě serverů Windows 2003/W2008, kde je tato funkce zapnuta standardně. Tato funkce musí být zapnuta alespoň pro základní události tj. úspěšná a neúspěšná přihlášení, restart serverů atd. Musí být zaznamenáváno i úspěšné přihlášení uživatelů. V současnosti se loguje pouze neúspěšné uživatelské přihlášení.
- Na všech serverech a klientech se při přihlašování automaticky zobrazuje login jméno naposledy přihlášeného uživatele. Tato vlastnost musí být vypnuta a doporučujeme modifikovat přihlašovací stránku o hlášení, že se uživatel přihlašuje k chráněnému systému a jeho činnost může být logována.

- Na serveru SERVERHP jsou nainstalovány certifikační služby a jejich konfigurace je ve sdíleném adresáři certconfig a certenroll s právem read pro skupinu EVERYONE. Tyto adresáře nesmí být sdílené.
- Na některých serverech je nainstalován a provozován databázový systém MS SQL 2005 pod systémovým účtem sa. Je nutné zajistit, aby tento účet používal vždy silné heslo. Klient s touto slabinou může být zneužit pro získání přístupu na další servery a klienty.
- Na serveru SERVERHP běží zbytečně služba SMTP. Tato služba musí být povolena pouze na Exchange serveru. Na všech ostatních serverech je nutné tuto službu zastavit, neboť hrozí zneužití této služby pro neautorizované odesílání mailů.
- Na některých klientech a serverech běží zbytečně služba SNMP. Vzhledem k tomu, že se nepoužívá trvalý dohled pomocí centrální SNMP konzoly měla by být tato služba zastavena. Další variantou je nainstalovat centrální konzoli např. MS System Center, z které by se prováděl dohled počítačů pomocí SNMP. V případě, že se nebude provádět trvalý dohled serverů a klientů z centrální konzoly doporučujeme tuto službu používat pouze na aktivních prvcích a monitorovaných serverech.
- Na klientech se používá služba NTP (port 123/UDP – časová služba), i když není nezbytně nutná. Doporučujeme tuto službu zastavit, protože může být využita k DDOS útoku.
- Na aktivních prvcích běží služby telnet, SNMP, občas http. U všech služeb je potřeba rozhodnout, jestli jsou nezbytně nutné a omezit jejich používání.
- Na některých aktivních prvcích běží zbytečně služba telnet a zároveň i služba http. Službu telnet je třeba vypnout a důsledně používat službu ssh, jestliže konfigurace zařízení tuto službu podporuje. SSH používá mechanismy pro šifrování hesel. Toto opatření se netýká starších aktivních prvků a komponent kde službu ssh nejde nasadit.
- Na serverech a klientech musí být vyhodnocovány bezpečnostní slabiny a aplikovány bezp. patche podle používaných služeb. Aplikování záplat sice probíhá automatizovaně, ale některé záplaty by měly být nasazeny co nejrychleji po otestování ve zkušebním prostředí. Je třeba vyhodnocovat kritické aktualizace, které nejsou distribuovány přes WSUS. Tuto kontrolu musí provádět správce alespoň 1x měsíčně.

- Na všech serverech musí být pravidelně provedena analýza hesel uživatelů pomocí specializovaných nástrojů např. Lophtcrack. V případě prolomení hesla musí být urychleně změněno uživatelem. Nesmí se používat slabá hesla kratší než 7 znaků.
- Neomezuje se přístup na WWW stránky přes proxy a uživatelé můžou stahovat libovolný obsah z Internetu. V případě, že pracovník použije anonymní proxy server např. www.shadowbrowser.com, pak nelze jeho činnost nijak kontrolovat. Během revize byly přístupné některé stránky s nepovoleným obsahem. Jako řešení lze použít nastavení DNS serveru z volně dostupné služby Secure DNS. Pak bude povolena jenom komunikace s WWW servery s nezávadným obsahem.
- Musí být zajištěna redundance služeb zejména DHCP a DNS. Výpadek serverů s těmito službami musí být nahrazen okamžitě záložním serverem. V současnosti je tato podmínka splněna pouze pro službu DNS, ale ne pro službu DHCP. Tento požadavek musí být zohledněn v plánu obnovy funkčnosti a služba DHCP musí být nakonfigurována i na záložním serveru v poměru přidělení IP adres 70:30.
- Během auditu byl na uživatelské stanici nalezen vir, který nedokázal detekovat a odstranit antivirový systém od AVG. Proto musí správce používat specializovaný sw. pro odstraňování virů od jiného dodavatele antivirových řešení.
- Pro zajištění větší míry záruk za zálohovací proces je nutné aplikovat systém shadow copies ve spolupráci s kvalitním zálohovacím nástrojem. Obnova a zálohování musí být součástí plánu obnovy. Zálohy musí být uloženy mimo místnost serverů.
- Infrastruktura sítě není plně odolná proti výpadkům a nedokáže eliminovat např. výpadek centrálního aktivního prvku Linksys nebo např. firewallu.
- Během průnikového testování byla ověřena možnost odposlechu síťové komunikace v LAN na použitých přepínačích. Všechny služby, které přenášejí nezašifrované hesla, jsou lehce odposlechnutelné z libovolného klienta vnitřní sítě. V případě, že uživatel použije stejné heslo do domény i do externí komunikace k WWW stránkám, pak může být narušena bezpečnost uživatelova účtu odposlechem na vnitřní síti. Tato hrozba bude snížena rekonfigurací VLAN a segmantací sítě, bez vzájemného proroutování. Pro aktivní prvky a jejich management musí být použita samostatná VLAN, která nebude směrována do dalších VLAN.
- Není používán žádny systém IDS/IPS na úrovni LAN. Lze řešit nasazením nového centrálního přepínače s podporou routování a funkcí filtrování provozu např. z řady

HP ProCurve 6400 nebo jiným prvkem do firmy CISCO. Lze řešit i nasazením samostatných boxů IDS/IPS např. řady Cisco 4200.

- Stávající přepínače nemají dostupné některé bezpečnostní funkce pro detekci síťových útoků typu spoofing source MAC adres apod. (Port Security, DHCP Snooping,
- Dynamic ARP Inspection, IP Source Guard). Doporučujeme nákup nového přepínače, který bude mít tyto bezpečnostní funkce. Na tento přepínač budou následně připojeny přepínače se servery a další přepínače pro klienty včetně firewallu.
- Na vybrané klienty (zejména notebooky a PC zajišťující styk s bankou) je nutno nasadit software pro šifrování dat na úrovni souborů a adresářů.
- Musí být zajištěno pronikání informace o bezpečnostním incidentu nebo nedostupnosti služby i v případě nedostupnosti správce. Není např. vyhodnocováno logování z firewallu Kerio. Logy je třeba zasílat na centrální stanici např. s MS Systém center.
- Na serverech běží zbytečně služby např. WZCSVC (bezdrátová zařízení) a DCOM, které nejsou nezbytně nutné pro činnost IS. Tyto služby nejsou nezbytně nutné a měly by být urychleně zastaveny, neboť mohou být zneužity pro DoS útoky.
- Služba POP3 musí být zrušena a nesmí být používána v prostředí Internetu. Je třeba ji nahradit zabezpečenou verzí nebo používat SSL

3.4 Stručné výsledky auditu

Celkový stav bezpečnosti IT v auditovaném podniku lze na základě ustálené běžné praxe hodnotit jako **dostatečný s výhradami**. Stávající bezpečnostní dokumentace společnosti nenaplňuje základní požadavky z pohledu koncového uživatele a neobsahuje všechny potřebné informace vyžadované bezpečnostními standardy. Neexistuje ucelená politika bezpečnosti IT a rovněž není vytvořen plán obnovy funkčnosti. Není zajištěna garance včasné obnovy jednotlivých částí IT.

Nejzávažnější nedostatky zjištěné auditem jsou popsány v následujících kapitolách. Jsou zde též uvedena základní doporučení pro nápravu tohoto stavu. Účelem této práce není pátrat po příčinách zjištěných nedostatků. Vzhledem ke komplexní provázanosti problematiky bezpečnosti jde řada popisovaných problémů za rámec informačních technologií a míří k širší problematice začlenění IS do celé organizace.

3.4.1 Hodnocení dokumentace

V rámci auditu byl zjištěn jako nejvážnější problém v nekomplexnosti bezpečnostní dokumentace. Neexistuje bezpečnostní politika IS, bezpečnostní směrnice IS a plán obnovy funkčnosti. Některé IT dokumenty obsahují pouze základní informace bez dalších návazností. V organizaci je zaveden formální systém školení zaměstnanců v oblasti bezpečnosti práce, do kterého spadá i používání a bezpečnost prostředků IT, ale uživatelé nemají dostatečné vědomosti o ochraně informací.

Vedením společnosti musí být aplikována bezpečnostní politika IS platná závazně v celé organizaci. Tato politika musí být závazná. Bezpečnostní politika IS by měla být vypracována dle ISO/IEC 27002 doplněné o problematiku Internetu např. v Site Security Handbook dle RFC2196 (nahrazující RFC1244). Další variantou je napsání vlastní politiky dle volně dostupných zdrojů na Internetu. Příkladem vhodného řešení je na http://www.boran.com/security/index.html tzv. IT Security Cookbook. Politiku lze napsat vlastními silami pro vybrané oblasti např. pouze pro informační systém, pouze pro fyzickou ochranu atd. Vhodnějším řešením bude vypracování této politiky nezávislou autoritou mimo organizaci.

Během revize byly poskytnuty dokumenty uvedené v následující tabulce. Získané materiály budou po provedení revize skartovány. Předané materiály byly hodnoceny na obsah a požadavky bezpečnosti IS. Většina dokumentu má pouze deklarativní charakter a neobsahuje přesný návod pro řešení konkrétních situací, takže běžný uživatel IS nemá možnost přesně pochopit, co má řešit v oblasti bezpečnosti IS a proč.

Označení	**Název**
Bez označení	Provozní řád počítačových učeben
Bez označení	Využití IT– pro zaměstnance
Bez označení	Pracovní smlouva
Bez označení	Dohoda o pracovní činnosti
Bez označení	Dohoda o provedení práce
Č.j. 2/2004/Ku	Legislativní pravidla pro vypracování směrnic
Bez označení	Spisový a skartační řád
Bez označení	Směrnice ředitele č. 4/2007 k využívání informačnímu systému Helios
Č.j. 3/2006/Ko	Směrnice ředitele o použití identifikační karty č. 3/2006/Ko
Č.j. 4/2006/Ko	Pokyn ředitele o provozním řádu IT centra

Tabulka č.1 – Předané dokumenty

V této dokumentaci se objevují požadavky na řešení některých bezpečnostních problémů např. volby hesla, antivirová kontrola atd. Tyto dokumenty, ale nelze považovat za bezpečnostní politiku a směrnice, protože zpravidla pouze definují minimální bezpečnostní zásady. Rovněž není vypracován plán obnovy funkčnosti IS, takže většina pracovníků v IT nemá představu o činnosti, kterou by museli provádět v případě havarijní situace. Pro naplnění a aplikování požadavků obecně závazných právních norem je v dalším textu proveden rozbor legislativních požadavků a jejich dopady na ochranu informací.

3.4.1.1 Využití IT – pro zaměstnance

Z hlediska požadavků na zajištění IBP je tento dokument zcela nedostačující a má pouze deklarativní charakter. Běžný uživatel po jeho přečtení nezíská představu o svých právech a povinnostech v oblasti bezpečnosti IT. Pouze některé citace naplňují částečně požadavky na definici zásad bezpečnostní politiky, ale jednotlivé definice jsou velice vágní a nejednoznačné. Dokument spojuje požadavky na bezpečnostní politiku a směrnice dohromady, což může vést k mylnému závěru, že co není pokryto tímto dokumentem, je v podstatě povoleno.

Tento dokument musí být zrevidován a přepracován do podoby realistické bezpečnostní politiky IT. Ve spolupráci s plánem obnovy funkčnosti bude tvořit základ bezpečnostní dokumentace IT ve společnosti.

3.4.1.2 Provozní řád počítačových učeben (pro zákazníky společnosti)

Tento dokument alespoň rámcové definuje bezpečnostní požadavky pro používání počítačových učeben. Stávající forma použití samostatného dokumentu pro účastníky školení je akceptovatelná i do budoucna, ale lepší varianta je mít jeden dokument s bezpečnostní politikou a druhý se směrnicemi. Běžný uživatel by měl číst pouze dokumenty bezpečnostní politika a směrnice. Velký počet dokumentů vede u uživatelů k dezorientaci a následnému ignorování.

- nikde není nadefinován požadavek na ochranu „citlivých“ informací v nadřazených dokumentech. Organizace nemá zaveden systém klasifikace dat, takže uživatel neví, přesně co je třeba chránit a jaké operace jsou povoleny nebo zakázány.
- Organizace musí jasně deklarovat možnost monitorovat činnosti uživatelů a kontrolovat jejich email komunikaci a přístup na Internet. Ideální řešení je modifikovat přihlašovací obrazovku, kde uživatel bude na tuto skutečnost upozorněn při každém přihlášení.
- V dokumentaci není nikde uveden legislativní rámec pro případné sankcionování uživatelů, jejichž činnost by vedla k vyzrazení citlivých informací např. personálních informací
- Uživatelé nemají povědomí a znalosti o existenci uvedených dokumentů.

3.4.1.3 Legislativní pravidla pro vypracování směrnic

Dokument definuje zásady pro označování dokumentů, ale některé dokumenty předané v rámci auditu žádné označení neměly. Dokument popisuje postup návrhu, vypracování a schvalování směrnic, závazný ve společnosti pro všechny řídící pracovníky. Tento dokument neexistuje. Obnova se opírá o externí dodavatele a zdroje. Doby na archivaci jsou rámcově uvedeny ve spisovém a skartačním řádu. Maximální doba archivace je 45 let. Běžné dokumenty jsou archivovány po dobu 5 let vyjímečně po dobu 10 let.

- nikde není nadefinován postup obnovy ze záloh a schéma zálohování. Součástí schématu zálohování by měla být i průměrná doba zálohování a obnovy dat a co je přesně zálohováno.
- Do obnovy nejsou zapojeni koncoví uživatelé. Každý z nich podle funkce by měl mít nadefinovánu činnost, kterou by vykonával během obnovy na svém pracovním zařazení. Musí se zohlednit možnost použití alternativních prostředků např. papírové evidence.

Závěr hodnocení stávající předané dokumentace:

Stávající systém právního pokrytí IBP je zcela nedostačující, neboť není vyčerpávající z hlediska existujících rizik a možných prostředků právní ochrany. Je tedy nutno zejména:

- **definovat bezpečnostní rizika** podle předmětu činnosti zaměstnavatele a podle konkrétní pracovní náplně každého zaměstnance, a to zcela vyčerpávajícím způsobem - jejich plným výčtem;
- **systemizovat** tato rizika z hlediska možných formálních prostředků jejich regulace (pracovní smlouva. Organizační řád, pracovní řád, bezpečnostní politika, bezpečnostní směrnice - obecně závazná nebo jen pro určitý okruh zaměstnanců…);
- **určit konkrétní obsah práv a povinností** zajišťujících vyloučení, minimalizaci bezpečnostních rizik
- vypracovat **ucelený systém právních norem** z hlediska jejich formálního označení, závaznosti, systemizace z hlediska závaznosti obecné a speciální, tj. i z hlediska jejich závaznosti pro konkrétní subjekt v případě kolize či nutnosti doplnění;

- **zapracovat** určená práva a povinnosti do takového systému zahrnujících všechna bezpečnostní rizika při práci s prostředky IBP;
- **zajistit formálně dokonalé i věcné působení norem IBP**, tj. zejména průkazné seznámení s normami při vzniku pracovního poměru a během jeho trvání.

Doporučení:

- Vypracovat dokument bezpečnostní politiky IT a vypracovat plán obnovy funkčnosti IT. Musí být rovněž vypracovány komplexní bezpečnostní směrnice pro uživatele v IS. Tyto dokumenty musí být dodatečně zpracovány na základě dokumentace závazně platné v rámci celé společnosti a musí zohlednit požadavky nadřízených norem.
- Dokumenty související s IS nejsou jednoznačně a jednotně označovány. Každý dokument musí nést identifikátor s klasifikací dokumentu. Žádný z dokumentů ve společnosti neřeší detailně klasifikaci dat. Tato oblast není v rámci společnosti uspokojivě řešena a klasifikace informací a aktiv musí být součástí bezpečnostní politiky organizace, aby byla zaručena vazba mezi technickými a organizačními opatřeními. V rámci společnosti není vypracováno standardní povinné označování dokumentů návěstím a nejsou označována ani důležitá aktiva související s provozem IS. V dokumentech je třeba v případě potřeby udávat i dobu utajení nebo dobu pro skartování.
- Data, dokumenty a aktiva zpracovávané nebo provozované v rámci společnosti musí být klasifikovány do jedné z následujících klasifikačních úrovní z hlediska utajení.

Veřejná / neklasifikovaná informace

Data v této úrovni jsou dostupná komukoliv bez dopadů na organizaci. Integrita dat není životně důležitá. Výpadek služeb je akceptovatelný. Do této skupiny patří většina stávajících informací.

Pouze pro vnitřní potřebu

Externí přístup k těmto datům a systémům musí být chráněn. V případě vyzrazení těchto informací na veřejnost nejsou následky pro organizaci kritické. Organizace může ztratit částečně svůj kredit na veřejnosti. Vnitřní přístupy k informacím jsou selektivní podle skupin uživatelů. Typickým příkladem informací této úrovně jsou přehledy IP adres, seznamy uživatelů, plán rozvoje, auditní záznamy, bezpečnostní slabiny IT atd.

Diskrétní

Data této úrovně jsou velmi citlivá a musí být chráněna v rámci organizace a před externím přístupem. Informace je určena jen pro definované uživatele. Přístup neautorizované osoby k těmto datům může způsobit organizaci operační neefektivnost, finanční ztráty, ztrátu prestiže atd. Integrita dat je životně důležitá. Typickou skupinou informací této úrovně jsou: informace o platech, personální údaje, informace o dodavatelích, smlouvy s dodavateli, výrobní postupy, projektové dokumentace atd.

Vedení společnosti by mělo přistoupit k zařazení informací a aktiv IS do jednotlivých klasifikačních úrovní, jak z hlediska dostupnosti, tak z hlediska utajení. Vzor pro rozdělení lze nalézt např. na http://www.boran.com/security/index.html viz sekce Classification.

Klasifikace aktiv je dlouhodobý proces a u tak rozsáhlé organizace, nemůže být provedena v časovém horizontu kratším než 1 rok. Stávající mechanismy ochrany jsou nedostatečné pro vyšší stupně klasifikovaných informací a musí být nasazeno řešení kryptografie zejména pro přenosné počítače.

3.5 Personální zajištění a kontrolní činnost

Za jeden z nejzávažnějších problémů lze považovat skutečnost, že existuje pouze 1 pracovník - správce, který je svou pracovní náplní dedikován pro udržování a rozvoj bezpečnosti IS. Další pracovníci vykonávají pouze operativní činnosti při údržbě IT prostředí. Problematika bezpečnosti je v současnosti fakticky řešena činnosti správce. Není

definována role bezpečnostního správce IT. V tomto uspořádání se však může lehce stát, že zodpovědnost za bezpečnost informací bude dána na okraj pracovních priorit vzhledem k velkému zatížení. Správce by měl mít definovány povinnosti na řešení bezpečnostní problematiky ve své působnosti v pracovní náplni. Z problematiky IT není nadefinován požadavek na dodržování a prosazování bezpečnostní politiky.

Doplňkovým řešením se jeví dedikování vlastníků informací popř. aplikačních správců, kteří ve své pracovní působnosti budou řešit ochranu svěřených informací. Mimo oddělení IS musí být definován další pracovník, který bude mít na starosti nezávislý dohled nad bezpečností. Na úrovni nejvyššího managementu musí být definován pracovník, který zajistí přidělení odpovídajících finančních prostředků na bezpečnost IS a nezávislý dohled nad bezpečností v celé organizaci. Tomuto pracovníkovi by měly být poskytovány informace o aktuálním stavu bezpečnosti. Bezpečnost musí mít definovaní zaměstnanci uvedenu v pracovní smlouvě a funkčních náplních.

Doporučení:

Určit vedoucího pracovníka mimo IS zodpovědného za bezpečnost IS. Do jeho povinností je nutno jasně definovat požadavek na provádění kontrolní, vyhodnocovací a monitorovací činnosti. Přesně vymezit pracovní povinnosti pracovníka IS vykonávajícího funkci správce popř. vlastníka informací a trvat na dodržování tohoto rozdělení v praxi. Definovat požadavky na ochranu informací a dodržování bezpečnostních zásad do pracovní smlouvy a ve funkčních náplních. Zajistit plnou zastupitelnost správce IT a jednoho dalšího pracovníka. Zajistit delegování zodpovědnosti za bezpečnost provozu IT na dalšího pracovníka IT.

3.6 Kontrolní činnost a řízení konfigurace

Existují komponenty, služby, aplikace a nástroje, které nejsou pod kontrolou správce IS a starají se o něj externí dodavatelé. Není zajištěn dostatečně systémový audit a dohled.

Správce provádí monitoring zdrojů IT, ale chybí ucelená koncepce komplexního systémového managementu a auditu s možností okamžité reakce na výskyt nežádaných událostí. Neexistuje okamžitá zpětná vazba pro pracovníky IT. Alespoň 1x ročně by měl být proveden nezávislý audit bezpečnosti všech klíčových komponent IT, zejména serverů a

stanic vedoucím pracovníkem společnosti mimo IT. K prosazení požadavků bezpečnostní politiky by měl být použit specializovaný nástroj např. Belarc Security Advisor.

Doporučení:

Je nutno zavést kontrolní činnost v IS především ve vztahu k citlivým datům dle navrhované klasifikace. Kontrolní činnost musí být prováděna pracovníky mimo IT. Pracovníci IT musí provádět trvalý centralizovaný monitoring IT komponent na základě schválených požadavků systémového auditu. Správce musí mít alespoň minimální zpětnou vazbu o aktuálním stavu bezpečnosti IT.

Je třeba maximálně využívat bezpečnostní vlastnosti stávajících komponent např. audit v operačních systémech, bezpečné konfigurace v komponentách (např. oddělené VLAN) atd. Aplikované bezpečnostní funkce nejsou plnohodnotně využívány. Musí být prováděn nezávislý audit všech komponent alespoň 1x ročně. Tyto funkce mohou být řešeny ve spolupráci s externími dodavateli.

3.7 Fyzická bezpečnost

Hlavní komponenty jsou uloženy v místnosti serverů. Centrálním monitoringem v budovách společnosti jsou trvale monitorovány některé parametry okolí např. požár, vstup do místnosti serverů kamerou. Některé parametry nejsou monitorovány přímo v rozvaděčích s IT komponentami např. vlhkost vzduchu. V místnosti serverů je umístěn hasební přístroj volně na zemi a není zavěšen dle normy. Nejsou splněny všechny požadavky na protipožární bezpečnost. V následujícím přehledu jsou uvedeny nejvážnější nedostatky z oblasti fyzické a organizační bezpečnosti:

- Nejsou odizolovány prostupy kabeláže do místností.
- Není zajištěno snímání požáru v místnosti severů.
- Kabeláž není přehledně rozmístěna a popsaná

Doporučení:

Místnost serverů vybavit automatickou detekci požáru. Zajistit zvýšení odolnosti proti požáru vytmelením všech prostupů do místností serverů použitím specializované hmoty od firmy Hilti. V místnosti zajistit dostatečný chladící výkon a cirkulaci vzduchu. Zajistit snadný přístup do všech rozvaděčů jen pro minimální množinu pracovníků. Popsat a zdokumentovat stávající kabeláž.

3.8 Celkové manažerské hodnocení

V následující kapitole je provedeno nezávislé hodnocení celého prostředí IS z manažerského pohledu. Nejzanedbanější oblasti je kromě obnovy funkčnosti, organizace bezpečnosti a bezpečnostní politika - protože ve společnosti není definována komplexní bezpečnostní politika a plán obnovy funkčnosti není vypracován vůbec. Proto musí být uvedeným oblastem věnována maximální pozornost.

U systému byla hodnocena také bezpečnost stávajících opatření organizace dle mezinárodně uznávaného standardu ISO/IEC 27002. Tato norma je rozdělena do 10 sekcí, ve kterých jsou umístěny skupiny obsahující množiny relevantních kontrol. Každá organizace se musí snažit dosáhnout plného aplikování těchto kontrol. Tato kapitola zobrazuje implementaci bezpečnostních kontrol ve společnosti. V každé sekci má být dosaženo minimálně 75% pro akceptovatelnost výsledků dané sekce. V následující tabulce je uveden přehled dosažených výsledků jednotlivých sekcí.

Číslo	Název sekce	Stav
1	Informační bezpečnostní politika	22%
2	Organizace bezpečnosti	17%
3	Klasifikace a kontrola aktiv	29%
4	Personální bezpečnost	42%
5	Fyzická bezpečnost a bezpečnost prostředí	59%
6	Management počítačů a sítí	56%
7	Systémová kontrola přístupu	46%
8	Systémový vývoj a údržba	38%
9	Plánování obnovy funkčnosti	15%
10	Vyhovění požadavkům norem	28%
	Přehled za všechny oblasti	37%

Tabulka č. 2 - Hodnocení jednotlivých oblastí dle normy ISO/IEC 27002

V rámci ČSN ISO/IEC 27002 jsou definované kontroly pokryty různou hodnotou detailnosti. Tato detailnost je pokryta počtem otázek spojených s danou kontrolou. Objektivnost stoupá s větším počtem otázek. Z tabulky je patrné, že bezpečnostní mechanismy ve společnosti nejsou na dostatečné úrovni v žádné oblasti a bezpečnost musí být urychleně řešena komplexem protiopatření. Technická opatření v IS jsou na dostatečné úrovni, ale bez náležitých doplňkových opatření v oblasti organizační bezpečnosti nemůžou být naplněna ani technická opatření. Vzhledem k tomu, že není bezpečnostní politika IS automaticky se v hodnocení ztrácí 25 procent ve všech oblastech. Výsledkem je, že i když je technická infrastruktura sítí a serverů na dostatečné úrovni, nejsou ani tyto oblasti z pohledu bezpečnosti dostatečně naplněny. Rovněž je výrazná absence plánu obnovy funkčnosti.

Proto musí být ve společnosti nasazena technická a organizační opatření, která zajistí naplnění požadavků normy ISO/IEC 27002. V této kapitole je tabulkovou formou proveden návrh klíčových opatření, která by měla být vrcholovým managementem společnosti aplikována formou klíčových projektů. Většina projektů má dopad na chod celé organizace, proto by měla být těmto projektům věnována mimořádná pozornost.

V následující tabulce je barvou označena kritičnost procesu a to následovně:

- Vysoká kritičnost – červeně
- Střední kritičnost – modře
- Nízká kritičnost – zeleně

ID	**Zjištěný stav**	**Návrh opatření**	**Dopady z nezavedení opatření nebo výhody a přínosy**
1.	Politika existuje pouze v omezené formě	Vytvoření bezpečnostní politiky IS	Nadefinování základních bezp. „ukazatelů“ tvoří základ všech návazných prací v oblasti bezpečnosti
2.	Nejsou	Definování osob pro	Nemožnost prosazení bezp.

	definovány role	podporu bezpečnostního managementu	opatření bez podpory lidských zdrojů
3.	Existují bezp. Směrnice pouze v omezené formě	Vypracování bezpečnostních směrnic pro uživatele IS	Definování bezpečnostních návyků pro všechny uživatele s důrazem na práci s heslem
4.	Neexistuje systém klasifikace informací	Zavedení povinného označování všech informací a dokumentů vyšších stupňů.	Možné vyzrazení informací neautorizované osobě
5.	Pouze částečně	Zdokumentování provozního stavu serverů, aktivních prvků, služeb, přidělených adres atd.	Ztráta kontroly o komponentách
6.	Jen minimálně	Školení všech zaměstnanců	Vyjasnění požadavků kladených na uživatele a zvýšení právního povědomí.
7.	Není garance za provozní podmínky	Zajištění provozního prostředí v místnosti serverů	Lepší garance provozu pro servery a aktivní prvky v serverovně
8.	Není adekvátní politika hesel	V doméně W2003 a aplikacích vynutit stejnou politiku hesel.	Možné zneužití uživatelova hesla. Vynutit délku hesla alespoň 7 znaků, měnit hesla co 3 měsíce a povolit maximálně 5 uživatelských pokusů.
9.	Neexistuje bezp. dohled	Centrální monitorování a prosazování bezpečnosti sítí se zpětnou vazbou ke	Zajištění prosazování bezp. auditu pomocí volně dostupných nástrojů např. MBSA, nasazením nástroje

		správci	MS system Center .
10.	Neprovádí se	Penetrační testování sítě LAN v pravidelných intervalech	Zvýšení míry důvěryhodnosti za připojení k síti. Najmout externí subjekt
11.	Konfigurace VLAN je nedostatečná	Využití nových bezpeč.funkcí v aktivních prvcích a podporu VLAN	Všechny VLAN musí vytvářet logicky oddělenou síť umožňující komunikaci pouze mezi definovanými segmenty.
12.	Neexistuje kontrola síťové vrstvy	Nasadit systém detekce narušení IDS/IPS na síťové vrstvě	Využít technologie firmy CISCO. (lze řešit společně s předchozím bodem a zakoupit aktivní prvek s firewall/IDS/IPS funkcionalitou)
13.	Neexistuje plán obnovy	Vypracování plánu obnovy	Stanovení postupu v případě nouzové situace pro jednotlivé pracovníky/role.
14.	Nepoužívá se bezpečnostní management	Zakoupit a nasadit prostředek pro bezpečnostní dohled klientů a serverů.	Bude instalován MS System Centre. Tento prostředek musí být spouštěn v pravidelných intervalech vůči odladěné politice.
15.	Neexistuje PKI infrastruktura	Zajištění šifrování na kritických PC a v přenosných počítačích	Zvýšení míry utajení na klientech aplikováním šifrování dat na discích použitím EFS.

Tabulka č. 3 - Tabulka s návrhem klíčových bezpečnostních opatření

3.9 Závěrečné doporučení pro management

Účelem tohoto dokumentu je zmapování stavu bezpečnosti IS. Z výše uvedených skutečností je možné konstatovat, že byly zjištěny základní nedostatky, které jsou shrnuty **v předchozích částech dokumentu**. Doporučujeme, společně s výše uvedeným, sladit strategické záměry společně s řešením návrhů na opatření vyplývající z tohoto dokumentu. Z provedené analýzy bylo provedeno hodnocení a posouzení klíčových nedostatků. Ty jsou shrnuty do následující tabulky. V této části dokumentu jsou uvedeny pro rychlejší orientaci a snadnější možnost opravy zjištěných nedostatků.

Číslo	Opatření
1.	Musí být definována organizační struktura pro práci s informacemi tak, aby bylo zajištěno odpovídající dělení povinností. Musí být definováni vlastníci informací, bezpečnostní správce a vedoucí pracovník mimo IT, který bude řešit problematiku bezpečnosti IT komplexně.
2.	Zástupce vrcholového managementu musí pravidelně vyhodnocovat bezpečnostní problematiku IS.
3.	Musí být definován další bezpečnostní správce částečně spoluzodpovědný za definovanou oblast IS (aplikace, servery Windows, aktivní prvky atd.).
4.	Musí být vypracován nový dokument realistické bezpečnostní politiky informačního systému.
5.	Musí být vypracován dokument bezpečnostních směrnic pro koncového uživatele IS.
6.	Musí být vypracován dokument „Plán obnovy IT“ zdrojů.
7.	Všechny systémy musí vynucovat shodnou politiku pro práci s hesly. Délka 7 znaků, změna každých 90 dnů, maximálně 5 neúspěšných přihlášení, historie hesel atd. Tyto zásady musí být nastaveny primárně v doméně W2003.
8.	Musí být přejmenovány všechny lehce předvídatelné systémové a

	uživatelské účty např. administrator, ftp atd.
9.	Musí být snížen počet sdílených adresářů a provedena revize přístupových práv. Logika použití sdílených adresářů musí být maximálně jednoduchá a přehledná. Musí být definováni jednotliví vlastníci, kteří rozhodují a použití přístupových práv k daným adresářům.
10.	Je nutno zabezpečit pravidelný audit konfigurace bezpečnosti Windows 2003/W2008 serverů. Zpočátku ručně nebo použitím standardních nástrojů v OS např. MBSA, GFI Languard atd.
11.	Alespoň 1x měsíčně musí být kontrolována konfigurace všech aplikací na serverech a typových klientech nezávislým posouzením např. pomocí Secunia Software inspektor dostupného na http://secunia.com/software_inspector. Na kontrolovaném počítači musí být nainstalována Java. Touto kontrolou jsou pokryty i aplikace třetích stran, které nejsou záplatovány přes službu WSUS. Kontrolu lze rovněž provádět pomocí profesionálních nástrojů např. Belarc Security Advisor.
12.	V systémech serverů musí být zapnut a pravidelně vyhodnocován bezp. audit pomocí doporučeného profesionálního nástroje. K dispozici je utilita Microsoft Baseline Security Analyzer nebo nové nástroje firmy Microsoft určené management a systémový dohled.
13.	Je třeba omezit počet služeb na serverech, které nejsou nutné pro vlastní provoz IS např. služba pro běh WiFI, bluetooth atd.
14.	Správce musí pravidelně kontrolovat systémové logy síťových uzlů a serverů ze systému např. pomocí MS Systém Center nebo obdobných.
15.	Správce systému musí pravidelně kontrolovat chybové logy na centrálních konzolách serverů a reagovat na tato hlášení. Doporučujeme integrovat zasílání logů na stanici správce např. do nástroje EventComb od Microsoft nebo sjednotit všechny logy na definovaném serveru s W2008, který již má integrováno sbírání logů.
16.	Musí být zajištěno trvale monitorování bezpečnosti s dostupnými nástroji.

	Musí být prováděna kontrola používaných systémových a bezpečnostních záplat v nástroji GFI Languard a MBSA pro celou doménu.
17.	Uživatelé musí dodržovat politiku pro správnou volbu hesel a musí s ní být seznámeni. Stávající délku hesla doporučujeme zvětšit alespoň na 7 znaků.
18.	Všechny systémy musí prosazovat stejnou politiku pro práci s heslem. Toto opatření se týká zejména kritických aplikací a Windows 2003 domény. Všechny servery musí mít obdobnou politiku hesel pro všechny uživatele kromě správce. Ten musí pro normální práci používat běžný uživatelský účet a přepínat se do administrátorského módu jenom při provádění administračních zásahů.
19.	Pravidelně musí být prováděna kontrola rozluštitelnosti hesel pomocí schváleného nástroje na serverech (např. LophtCrack).
20.	Musí být prováděno monitorování veřejného IP adresního prostoru včetně průnikových testů alespoň 2x ročně.
21.	Musí byt provedena logická segmentace sítí pomocí ACL a ratingu pro samostatné VLAN oddělující segment serverů a klientů. Klienti jedné sítě nesmí mít možnost ohrozit provoz v dalších částech sítě.
22.	Musí být nasazen systém pro detekci narušení IDS/IPS pracující na síťové vrstvě, nejlépe od firmy CISCO např. Cisco 4200, Cisco 2800. Jde využít i jiných dodavatelských řešení.
23.	Vypravovat nový koncept zálohování a zajistit ukládání dat ve druhé budově mimo místnost pořízení.
24.	Vypracovat plán obnovy funkčnosti zajišťující dostupnost sítě, Internetu a serverů do 48 hodin.
25.	Zajistit dostupnost Internetu jiným fyzickým spojením nejlépe k jinému poskytovateli.
26.	Zajistit pro všechny servery reakci od dodavatele v úrovni „Next Business Day“.

27.	Správce musí dostat 1 licenci pro antivirový a antispamový software zahraniční provenience. Tímto softwarem se budou ověřovat poplachy signalizované používaným antivirovým softwarem. Ten je v současnosti měněn z AVG na řešení od společnosti MS.
28.	Není řešena redundance IP adres přidělovaných přes DHCP. V lokalitě Praha musí být tato služba nadefinována alespoň na 2 serverech. Změna byla řešena v průběhu auditu. Dalším řešením je zajištění primárního přidělování IP adres z DHCP na aktivním prvku.
29.	Zajistit dostupnost záloh konfigurací jednotlivých komponent síťové infrastruktury (např. zálohování konfigurací a sledování změn pomocí nástroje CatTools).
30.	Provádět pravidelný update verzí operačního systému na jednotlivých prvcích síťové infrastruktury po náležitém otestování. Používat nové bezpečnostní prvky dostupné v nových verzích IOS.
31.	Pro správu aktivních prvků síťové infrastruktury používat protokol ssh, doplnit ACL povolující správu jen z vyhrazených adres, zakázat služby telnet a WWW management.
32.	Na úrovni VPN používat spojení L2TP s certifikátem vydaným lokální certifikační autoritou
33.	Na firewallu Kerio aplikovat tvrdší kontrolu přístupu k WWW stránkám nebo používat DNS službu ze zabezpečených 3 stran např. z www.opendns.org.

Tabulka č.4 - Návrh detailních opatření pro zvýšení bezpečnosti v IT

3.10 Rekapitulace závěrů pro management

V následujícím přehledu je uveden seznam globálních závěrů bezpečnostního auditu provedeném ve společnosti za oblast bezpečnosti informačních technologií:

1) Velké nedostatky jsou v organizačním zabezpečení činnosti IS ve společnosti. Není vypracována realistická bezpečnostní politika informačního systému. Rovněž je nutné přepracovat a doplnit stávající bezpečnostní dokumentaci pro uživatele. Plán obnovy IT zdrojů musí být rovněž vypracován jako samostatný dokument a musí být doplněn o konkrétní obnovovací procedury. Neexistuje systém klasifikace dat.

2) Oblast zajištění zodpovědnosti za informace v IS je nedostatečná a je nutno urychleně vypracovat postupy pro přidělení odpovědnosti za informace, přidělení pouze nezbytně nutných práv k objektům dle stupně klasifikace atd. Dále je nutno vypracovat dělení zodpovědnosti za problematiku bezpečnosti informací v celé společnosti a v IS definováním vlastníků informací. Ve vrcholovém managementu musí být definován pracovník zodpovědný za bezpečnost IS. Správce a jeho zodpovědnosti musí být zálohovány druhou pověřenou osobou, která bude vykonávat funkci bezpečnostního správce.

3) Pro vyšší stupeň utajení (stupeň „Diskrétní“) citlivých dat **NEJSOU** stávající prostředky zpracování dostatečné a je nutno používat nadstandardních technik např. šifrování dat na kritických PC a přenosných počítačích. Je nutné zakoupit doplňkový software.

4) Analýza provozního prostředí IT ve společnosti ukázala, že velké nedostatky lze hledat v nedostatečném využívání bezpečnostních opatření v již používaných technologiích. Důraz musí být kladen na využití prostředků pro management systému a aktivních prvků zejména pomocí standardních prostředků dostupných v OS a v doméně W2003. Všichni klienti by měli být na platformě Windows XP a všechny servery na platformě Windows 2003/W2008. Na auditorské stanici je nainstalována sada programů pro provádění základní bezpečnostní kontroly všech prvků sítě. K dispozici je i profesionální bezpečnostní scanner Languard firmy GFI a další.

5) Musí být zajištěno monitorování dostupnosti sítě a serverů např. pomocí nástrojů firmy Microsoft zpětnou vazbou pro správce. V rámci auditu byly použity doplňující softwarové nástroje pro management a monitorování bezpečnosti např. Belarc Security

Advisor. Tento software by měl být pravidelně používán nejenom správcem, ale i pověřenou osobou z vrcholového managementu. Kontrola této činnosti musí být prováděna vedoucím pracovníkem mimo IS.

6) V době auditu nebyla uspokojivě řešena oblast obnovy funkčnosti a zálohování. Urychleně musí být zahájeny práce na vypracování plánu obnovy klíčových aktiv IS doplněném o konkrétní obnovovací procedury a postupy. Musí být procvičeny a otestovány jednotlivé obnovovací procedury po odladění nového zálohovacího schématu s novou verzí MS data recovery doplněného mechanismem shadow copies na úrovni operačního systému serverů spouštěném 4x denně.

7) Musí být provedena logická segmentace sítí pomocí ACL a routingu pro samostatné VLAN oddělující segment serverů a segmenty klientů. Musí být nasazen systém pro detekci narušení IDS/IPS pracující na síťové vrstvě, nejlépe od firmy CISCO např. Cisco 4200, Cisco 2800. Rovněž musí být zajištěna dostupnost internetu jiným fyzickým médiem mimo stávající optické spoje.

8) Musí být nadefinována a prosazena optimální politika pro práci s hesly. Tato politika musí být vynucována ve všech systémech shodně tak, aby si ji uživatel lehce pamatoval. Délka hesla musí být alespoň 7 znaků a v doméně W2003 musí být zapnut parametr na dodržování komplexity hesel. Hesla musí být měněna alespoň 1x 3 měsíce a systémy musí povolit maximálně 5 uživatelských pokusů o přihlášení. Pak musí být uživatelův účet zamknut na 30 minut. Nesmí být používány snadno předvidatelné účty např.*nazev_firmy, ftp* atd. Uživatelské jméno dříve přihlášeného uživatele nesmí být zobrazováno v přihlašovací obrazovce a uživatel je musí zadávat manuálně, při každém přihlášení.

ZÁVĚR

Realizace bezpečnostního auditu IT ve vybraném podniku nebyla typickou ukázkou práce na certifikaci systému nebo na její kontrole. Návody a postupy uvedené v prezentovaných normách jsou však uplatnitelné i jednotlivě a odděleně od procesu certifikace či analýzy souladu s normou. V případě auditovaného podniku šlo o plnění konkrétního zadání, které nezahrnovalo ani zmínku o řízení bezpečnosti. Nicméně hledání příčiny vzniku zákazníkových potíží někdy vede k odhalení systémové chyby nebo potřeby zavedení procesu řízení bezpečnosti nebo řízení informací obecně. I zde šlo o klasický případ, v praxi se tak často opakující, kdy řešení konkrétních problémů ukáže na bolavá místa a nastaví správný směr vývoje v oblasti bezpečnosti a tvorby IS. Stejně tak v tomto případě směřovala mnohá doporučení k úpravě procesu, ne pouze k zalátání bezpečnostních děr. Požadavek na analýzu vznikl, jako potřeba ochrany investic při zavádění jednoho z výše uvedených systémů. Zadání projektu bylo nakonec splněno. Co je ale v tomto případě nejdůležitější, je fakt, že auditovaný podnik začal na potřebu řízení bezpečnosti nahlížet jako nutnost pro fungování organizace. To je ten první správný krok, který dlouhodobě vede k úsporám a benefitům konkurenční výhody – bezpečné práce s informacemi a bezvadného IS.

ZÁVĚR V ANGLIČTINĚ

Realization of security audit in the specific company was not a typical case of work on system certification or it's verification. Suggestions and methods mentioned in presented norms are, however, useable even individually outside the certification process or the analysis of conformity with the norm. In the case of audited company there was not a mention of security management in the specific project definition. However, the process of searching for the reason of customer's specific problems sometimes lead us to discovery of a system fault or need of implementation of security management process or information management generally. Even in our case we've met a classical situation where process of solving specific problems discovers "sore spots" and helps to set the right direction of development in the area of IS security and creation. Also in this described case many suggestions lead to changes in processes rather than just fixing already known particular errors. The request for analysis raised from the need of protection of investments during implementation of one of mentioned systems. The definition of the project was finally fulfilled. The most important result of the project, however, is the fact, that audited company became to perceive the security management as necessary for company existence. This is the first good step towards the benefits of secure work with information and perfect IS.

SEZNAM POUŽITÉ LITERATURY

[1] ČSN ISO/IEC 27001:2006, Informační technologie – Bezpečnostní techniky – Systém managementu bezpečnosti informací – Požadavky.

[2] ČSN ISO/IEC 27002:2006, Informační technologie – Soubor postupů pro management bezpečnosti informací.

[3] ISO/IEC 27004, Information technology – Security techniques – Information security management measurements

[4] ISO/IEC 27006: 2007 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management system

[5] ISO/IEC 27005: 2008 – Information technology – Security techniques – Information security risk management

[6] KOPÁČIK, Ivan, et al. *Management and audit of Information security : Manual for Manager*. Brtatislava, Slovensko : Sineal s.r.o., 2007. 322 s. ISBN 978-80-969747-0-2.

[7] DOSEDĚL , Tomáš. *Počítačová bezpečnost a ochrana dat*. Libor Pácl. Brno : Computer press, c2004. 187 s. ISBN 80-251-0106-1.

[8] DOUCEK, P.: Bezpečnost informační systémů a její prosazování v České republice, In: Informatika 2003, pp. 141 – 146, Bratislava 2003, ISBN 80-233-0491-7.

[9] SVATÁ, V.: Audit informačního systému, VŠE Praha, 2007, ISBN 80-245-0975-X

POUR, Jan. *Informační systémy a technologie*. 1.vyd Edice učebních textů 2006. ISBN 80-86730-03-4

[10] VRANA, Ivan a RICHTA, Karel. *Zásady a postupy zavádění podnikových informačních systémů: Praktická příručka pro podnikové manažery*. 1. vyd. Praha : Grada, 2005. 187 s. ISBN 80-247-1103-6

[11] HANÁČEK, Petr a STAUDEK, Jan. *Bezpečnost informačních systémů,* Úřad pro státní bezpečnostní systém 2000

[12] MOLNÁR, Zdeněk. *Automatizované informační systémy*. Praha: ČVUT 2000, PLU 2607

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ISMS	Information security management system
PDCA	Plan, Do, Checkt, Act
IRH	Incident Response Handling
BIA	Disaster Response System
ACL	Access Control List (přístupové seznamy)
AD	Active Directory (adresářová služba Microsoftu)
BRP	Business Risk Profile
DC	Domain Controler – řadič domény
DG	Default gateway
DNS	Domain Name System
EPS	Elektronická požární signalizace
ERP	Podnikový systém
EZS	Elektronická zabezpečovací signalizace
FTP	File transfer protokol
GPO	Group Policy pro centrální management komponent domény W2003/W2008
HW	Hardware
IBP	Informační bezpečnostní politika
IDS/IPS	Intrusion Detection System (systém detekce narušení)
IBP	Informační bezpečnostní politika
IOS	Operační sytém v aktivních prvcích firmy CISCO
IS	Informační systém
ISP	Internet Service Provider
IPT	IP telefonie
IT	Informační technologie

MBSA	Microsoft Baseline Security Analyzer
NAT	Network Address Translation (překlad adres)
NBK	Notebook, přenosný počítač
NDA	Non Disclosure Agreement
SLA	Service Level Agreement – definice poskytovaných služeb v oblasti IT
SNMP	Simple network management protokol
SW	Software
TS	Terminálové služby
VNC	Software pro vzdálenou administraci firmy AT&T
WSUS	Windows Update Server
ZP	Zákoník práce

SEZNAM OBRÁZKŮ

SEZNAM TABULEK